```
### Status: Path 1 of [Dialog Information Services via Modem]

### Status: Initializing TCP/IP using (UseTelnetProto 1 ServiceID pto-dialog)
Trying 3106900061...Open

DIALOG INFORMATION SERVICES
PLEASE LOGON:
 ******** HHHHHHHH SSSSSSSS?
### Status: Signing onto Dialog
 ********
ENTER PASSWORD:
 ******** HHHHHHHH SSSSSSSS? ********
Welcome to DIALOG
### Status: Connected


Dialog level 01.07.09D

Last logoff:  30jul01 13:19:13
Logon file405 06aug01 13:27:54
           *** ANNOUNCEMENT ***
                    ***
--Important Notice to Freelance Authors--
See HELP FREELANCE for more information
                    ***
NEW FILE RELEASED
***EIU Business Magazines (File 622)
***IBISWorld Market Research (File 753)
***Investext PDF Index (File 745)
***Daily and Sunday Telegraph (London) Papers (File 756)
***The Mirror Group Publications (United Kingdom) (File 757)

UPDATING RESUMED
***Delphes European Business (File 481)
***Books In Print (File 470)
                           ***
RELOADED
***Kompass Middle East/Africa/Mediterranean (File 585)
***Kompass Asia/Pacific (File 592)
***Kompass Central/Eastern Europe (File 593)
***Kompass Canada (File 594)

New pricing structure for Pharmaprojects (Files 128/928) from
April 1, 2001. Check Help News128 or Help News928 for further
information.

>>>Get immediate news with Dialog's First Release
   news service.  First Release updates major newswire
   databases within 15 minutes of transmission over the
   wire.  First Release provides full Dialog searchability
   and full-text features.  To search First Release files in
   OneSearch simply BEGIN FIRST for coverage from Dialog's
   broad spectrum of news wires.

     >>> Enter BEGIN HOMEBASE for Dialog Announcements <<<
     >>>    of new databases, price changes, etc.      <<<
                    ****
COREFULL is set ON as an alias for 15,9,623,810,275,624,636,621,813,16,160,148,20.
COREABS is set ON as an alias for 77,35,593,65,2,233,99,473,474,475.
COREALL is set ON as an alias for COREFULL,COREABS.
SOFTFULL is set ON as an alias for 278,634,256.
EUROFULL is set ON as an alias for 348,349.
JAPOABS is set ON as an alias for 347.
HEALTHFULL is set ON as an alias for 442,149,43,444.
HEALTHABS is set ON as an alias for 5,73,151,155,34,434.
DRUGFULL is set ON as an alias for 455,129,130.
```

```
DRUGABS is set ON as an alias for 74,42.
INSURANCEFULL is set ON as an alias for 625,637.
INSURANCEABS is set ON as an alias for 169.
TRANSPORTFULL is set ON as an alias for 80,637.
TRANSPORTABS is set ON as an alias for 108,6,63.
ADVERTISINGFULL is set ON as an alias for 635,570,PAPERSMJ,PAPERSEU.
INVENTORYABS is set ON as an alias for 8,14,94,6,34,434,7.
BANKINGFULL is set ON as an alias for 625,268,626,267.
BANKINGABS is set ON as an alias for 139.
HEALTHALL is set ON as an alias for COREFULL,COREABS,HEALTHFULL,HEALTHABS.
INSURANCEALL is set ON as an alias for COREFULL,COREABS,INSURANCEFULL,INSURANCEABS.
RESERVATIONALL is set ON as an alias for COREFULL, COREABS.
OPERATIONSALL is set ON as an alias for COREFULL,COREABS,INVENTORYABS.
TRANSPORTALL is set ON as an alias for COREFULL,COREABS,TRANSPORTFULL,TRANSPORTABS.
ADVERTISINGALL is set ON as an alias for COREFULL,COREABS,ADVERTISINGFULL.
SHOPPINGALL is set ON as an alias for COREFULL,COREABS,ADVERTISINGALL,47.
INVENTORYALL is set ON as an alias for COREFULL,COREABS,INVENTORYFULL.
BANKINGALL is set ON as an alias for COREFULL,COREABS,BANKINGFULL,BANKINGABS.
PORTFOLIOALL is set ON as an alias for COREFULL,COREABS,BANKINGALL.
TRADINGALL is set ON as an alias for COREFULL,COREABS,BANKINGALL.
CREDITALL is set ON as an alias for COREFULL,COREABS,BANKINGALL.
FUNDSALL is set ON as an alias for COREFULL,COREABS,BANKINGALL,608.
SYSTEM:HOME
Menu System II: D2 version 1.7.8 term=ASCII
                    *** DIALOG HOMEBASE(SM) Main Menu ***

 Information:
  1.  Announcements (new files, reloads, etc.)
  2.  Database, Rates, & Command Descriptions
  3.  Help in Choosing Databases for Your Topic
  4.  Customer Services (telephone assistance, training, seminars, etc.)
  5.  Product Descriptions

 Connections:
  6.  DIALOG(R) Document Delivery
  7.  Data Star(R)

    (c) 2000  The Dialog Corporation plc      All rights reserved.

      /H = Help            /L = Logoff          /NOMENU = Command Mode


Enter an option number to view information or to connect to an online
 service.  Enter a BEGIN command plus a file number to search a database
(e.g., B1 for ERIC).
?b corefull, coreabs

       06aug01 13:28:08 User242933 Session D52.1
            $0.00    0.200 DialUnits FileHomeBase
     $0.00  Estimated cost FileHomeBase
     $0.01  TYMNET
     $0.01  Estimated cost this search
     $0.01  Estimated total session cost   0.200 DialUnits


SYSTEM:OS  - DIALOG OneSearch
  File  15:ABI/Inform(R)  1971-2001/Aug 04
         (c) 2001 ProQuest Info&Learning
  File   9:Business & Industry(R)  Jul/1994-2001/Aug 03
         (c) 2001 Resp. DB Svcs.
  File 623:Business Week  1985-2001/Aug W1
         (c) 2001 The McGraw-Hill Companies Inc
  File 810:Business Wire  1986-1999/Feb 28
         (c) 1999 Business Wire
  File 275:Gale Group Computer DB(TM)  1983-2001/Aug 02
         (c) 2001 The Gale Group
  File 624:McGraw-Hill Publications  1985-2001/Aug 03
```

(c) 2001 McGraw-Hill Co. Inc
File 636:Gale Group Newsletter DB(TM) 1987-2001/Aug 03
(c) 2001 The Gale Group
File 621:Gale Group New Prod.Annou.(R) 1985-2001/Aug 03
(c) 2001 The Gale Group
File 813:PR Newswire 1987-1999/Apr 30
(c) 1999 PR Newswire Association Inc
File 16:Gale Group PROMT(R) 1990-2001/Aug 03
(c) 2001 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
(c) 1999 The Gale Group
File 148:Gale Group Trade & Industry DB 1976-2001/Aug 03
(c)2001 The Gale Group
File 20:World Reporter 1997-2001/Aug 06
(c) 2001 The Dialog Corporation
***File 20: Duplicate Detection has been restored to file 20.**
File 77:Conference Papers Index 1973-2001/Jul
(c) 2001 Cambridge Sci Abs
File 35:Dissertation Abs Online 1861-2001/Jul
(c) 2001 ProQuest Info&Learning
File 593:KOMPASS Central/Eastern Europe 2001/Jul
(c) 2001 KOMPASS Intl.
File 65:Inside Conferences 1993-2001/Aug W1
(c) 2001 BLDSC all rts. reserv.
***File 65: For variance in UDs please see Help News65.**
File 2:INSPEC 1969-2001/Aug W1
(c) 2001 Institution of Electrical Engineers
File 233:Internet & Personal Comp. Abs. 1981-2001/Aug
(c) 2001 Info. Today Inc.
File 99:Wilson Appl. Sci & Tech Abs 1983-2001/Jun
(c) 2001 The HW Wilson Co.
File 473:FINANCIAL TIMES ABSTRACTS 1998-2001/APR 02
(c) 2001 THE NEW YORK TIMES
***File 473: This file will not update after March 31, 2001.**
It will remain on Dialog as a closed file.
File 474:New York Times Abs 1969-2001/Aug 04
(c) 2001 The New York Times
File 475:Wall Street Journal Abs 1973-2001/Aug 06
(c) 2001 The New York Times

Set	Items	Description

?s (certificate) and (public or private or secret) and (key or keys) and (fragment or c
ount or date or meter or value or amount or weight or size or register or zip or zipcod
e) and (indicia or indicium) and (postal or postage)
Processing
Processed 10 of 23 files ...
Processing
Processed 20 of 23 files ...
Completed processing all files

230554	CERTIFICATE
7606694	PUBLIC
3467291	PRIVATE
375999	SECRET
3834412	KEY
195542	KEYS
45323	FRAGMENT
636812	COUNT
2907408	DATE
193258	METER
4750746	VALUE
2480666	AMOUNT
695126	WEIGHT
2466242	SIZE
508066	REGISTER
88197	ZIP
1299	ZIPCODE

```
          2760  INDICIA
           149  INDICIUM
        183218  POSTAL
         54813  POSTAGE
S1         40  (CERTIFICATE) AND (PUBLIC OR PRIVATE OR SECRET) AND (KEY
               OR KEYS) AND (FRAGMENT OR COUNT OR DATE OR METER OR VALUE
               OR AMOUNT OR WEIGHT OR SIZE OR REGISTER OR ZIP OR
               ZIPCODE) AND (INDICIA OR INDICIUM) AND (POSTAL OR
               POSTAGE)
?s s1 and meter
           40  S1
       193258  METER
S2         15  S1 AND METER
?type s2/3,abs/all
>>>"ABS" is not a valid format name in file(s): 2, 9, 15-16, 20, 35, 65,
   77, 99, 148, 160, 233, 275, 473-475, 593, 621, 623-624, 636, 810, 813
?type s2/3,ab/all
>>>No matching display code(s) found in file(s): 65, 593, 623-624, 810, 813
```

2/3,AB/1 (Item 1 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01779500 04-30491
Stamping out crime
Bruno, Lee
Data Communications v28n2 PP: 16 Feb 1999 ISSN: 0363-6399 JRNL CODE: DCM
WORD COUNT: 189

ABSTRACT: Counterfeiters have been messing with **postal** meters, ripping off the US **Postal** Service to the tune of $100 million a year. But PKI (**public key** infrastructure) technology could help staunch the flow of illicit dollars - and let customers buy **postage** online.

2/3,AB/2 (Item 1 from file: 9)
DIALOG(R)File 9:Business & Industry(R)

02236322
USPS To Use PKI To Offer Electronic Postage
(US Postal **Service moves closer to selling** postage **online after establishing** public- key **infrastructure; service will use PKI as part of Information-Based** Indicia **Program)**
Newsbytes News Network, p N/A
September 10, 1998
DOCUMENT TYPE: Journal ISSN: 0983-1592 (United States)
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 528

ABSTRACT:
The US **Postal** Service is moving toward selling **postage** online, having set up a **public -key** infrastructure in 8/98. PKI will be used as part of the Information-Based **Indicia** Program (IBIP), which sells **postage** via the Internet, letting users print bar codes on envelopes or labels from printers at their home offices or in small businesses. Each of the digital stamps consists of a bar code that has unique, scannable data. The US **Postal** Service is losing about $100 mil per year due to **meter** tampering, according to **postal** officials. Meters represent some $21 bil per year in revenues. Cylink Corp (Sunnyvale, CA) provided the PKI system, which will create authorization certificates, audit transactions and recover interrupted transactions and revoke certificates. The full text further discusses the topic.

2/3,AB/3 (Item 1 from file: 810)
DIALOG(R)File 810:Business Wire
(c) 1999 Business Wire . All rts. reserv.

0793949 BW0360

SPYRUS: SPYRUS Unveils New Desktop Security for Electronic Postage **Metering**

January 12, 1998

Byline: Business Editors and High-Tech Writers

2/3,AB/4 (Item 1 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2001 The Gale Group. All rts. reserv.

02221072 SUPPLIER NUMBER: 21154848 (USE FORMAT 7 OR 9 FOR FULL TEXT)
USPS To Use PKI To Offer Electronic Postage **09/10/98.**
Newsbytes, n95, pNA
Sept 10, 1998
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 562 LINE COUNT: 00050

2/3,AB/5 (Item 2 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2001 The Gale Group. All rts. reserv.

02218111 SUPPLIER NUMBER: 21128822 (USE FORMAT 7 OR 9 FOR FULL TEXT)
USPS will use a PKI to manage electronic postage.(public key **infrastructure for** Postal **Service's** Indicia **program) (Government Activity)**
Mayer, Merry
Government Computer News, v17, n29, p14(1)
Sept 7, 1998
ISSN: 0738-4300 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 538 LINE COUNT: 00047

2/3,AB/6 (Item 3 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2001 The Gale Group. All rts. reserv.

02197540 SUPPLIER NUMBER: 20912092 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Stamping Out Fraud.(US Postal **Service is creating digital certificates for** postage **metering machines) (Government Activity)**
Kerstetter, Jim
PC Week, v15, n28, p14(1)
July 13, 1998
ISSN: 0740-1604 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 402 LINE COUNT: 00035

2/3,AB/7 (Item 1 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)
(c) 2001 The Gale Group. All rts. reserv.

03951852 Supplier Number: 50295217
USPS To Use PKI To Offer Electronic Postage **09/10/98**
Newsbytes, pN/A
Sept 10, 1998
Language: English Record Type: Fulltext
Article Type: Article
Document Type: Newswire; General Trade
Word Count: 536

2/3,AB/8 (Item 2 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)

03801533 Supplier Number: 48242468
HOBBY MARKETS ONLINE AUCTIONS PUT AVID DEALERS, COLLECTORS IN TOUCH WITH EACH OTHER
Information & Interactive Services Report, v19, n2, pN/A
Jan 23, 1998
Language: English Record Type: Fulltext
Document Type: Newsletter; Trade
Word Count: 1463

2/3,AB/9 (Item 1 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

01597722 Supplier Number: 48218951
SPYRUS Unveils New Desktop Security for Electronic Postage **Metering.**
Business Wire, p01120360
Jan 12, 1998
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 897

2/3,AB/10 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

06120131 Supplier Number: 53735690
Stamping Out Crime.(US Postal **Service selling stamps over Internet)(Government Activity)**
Bruno, Lee
Data Communications, p16(1)
Feb 7, 1999
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 194

2/3,AB/11 (Item 2 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

05802940 Supplier Number: 50295217
USPS To Use PKI To Offer Electronic Postage **09/10/98**
Newsbytes, pN/A
Sept 10, 1998
Language: English Record Type: Fulltext
Article Type: Article
Document Type: Newswire; General Trade
Word Count: 536

2/3,AB/12 (Item 3 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

05418087 Supplier Number: 48218951
SPYRUS Unveils New Desktop Security for Electronic Postage **Metering.**
Business Wire, p01120360
Jan 12, 1998
Language: English Record Type: Fulltext

Document Type: Newswire; Trade
Word Count: 897

2/3,AB/13 (Item 1 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2001 The Gale Group. All rts. reserv.

10459804 SUPPLIER NUMBER: 21128822 (USE FORMAT 7 OR 9 FOR FULL TEXT)
USPS will use a PKI to manage electronic postage.(public key **infrastructure for** Postal **Service's** Indicia **program) (Government Activity)**
Mayer, Merry
Government Computer News, v17, n29, p14(1)
Sept 7, 1998
ISSN: 0738-4300 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 538 LINE COUNT: 00047

2/3,AB/14 (Item 2 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2001 The Gale Group. All rts. reserv.

10322918 SUPPLIER NUMBER: 20912092 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Stamping Out Fraud.(US Postal **Service is creating digital certificates for** postage **metering machines) (Government Activity)**
Kerstetter, Jim
PC Week, v15, n28, p14(1)
July 13, 1998
ISSN: 0740-1604 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 402 LINE COUNT: 00035

2/3,AB/15 (Item 1 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.
(c) 2001 Info. Today Inc. All rts. reserv.

00501510 98PK07-107
Stamping out fraud -- Postal **Service will use certificates to curb** meter **malfeasance**
Kerstetter, Jim
PC WEEK , July 13, 1998 , v15 n28 p14, 1 Page(s)
ISSN: 0740-1604
Reports that the U.S. **Postal** Service will announce that it is building a **public - key** infrastructure (PKI) for its Information Based **Indicia** Program (IBIP), a plan to create digital certificates for **postage** metering machines. Reports that Cylink Corp. of Sunnyvale, CA, has built the PKI for the **Postal** Service and will host a pilot project in northern Virginia and the San Francisco Bay area. States that Cylink is using X.509 Version 3 certificates for the **Postal** PKI, which will be running off a SPARC-based server. Notes that while **Postal** officials are quiet, there is speculation that the IBIP is the first step toward the creation of a long-awaited **Postal** Service-run **certificate** authority, though notes such plans were discussed once before and set aside. Includes one screen display. (bjp)
July 13, 1998
?type s2/3,kwic/all
>>>KWIC option is not available in file(s): 77

2/3,KWIC/1 (Item 1 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)
(c) 2001 ProQuest Info&Learning. All rts. reserv.

01779500 04-30491
Stamping out crime
Bruno, Lee
Data Communications v28n2 PP: 16 Feb 1999

ISSN: 0363-6399 JRNL CODE: DCM
WORD COUNT: 189

ABSTRACT: Counterfeiters have been messing with **postal** meters, ripping off the US **Postal** Service to the tune of $100 million a year. But PKI (**public key** infrastructure) technology could help staunch the flow of illicit dollars - and let customers buy **postage** online.
TEXT: COUNTERFEITERS HAVE been messing with **postal** meters, ripping off the U.S. **Postal** Service (Washington, D.C.) to the tune of $100 million a year. But PKI (**public key** infrastructure) technology could help staunch the flow of illicit dollars-and let customers buy **postage** online. The Information Based **Indicia** Program (IBIP) from the U.S. **Postal** Service lets owners of special digital meters download

postage over the Internet. Its PKI server issues each **meter** a digital **certificate** that authenticates the device, and end-users can then print the **postage** on envelopes in the form of bar codes. Eventually, the **postal** service wants to start downloading **postage** directly to desktop PCs, allowing users to run out the bar codes via networked printers. The PKI for the U.S. **Postal** Service is scalable enough to generate and manage 300 million certificates. Developed by Cylink Corp. (Sunnyvale, Calif.), it's now housed at the vendor's

headquarters, but the U.S. **Postal** Service will take charge of it in the next few months.. Related 'Net-ready products already are starting to show: Estamp Inc. (Palo Alto, Calif.) is now selling $300 **postage** meters with bundled digital certificates. -Lee Bruno (San Mateo, Calif.)....

DESCRIPTORS: **Postal** & delivery services...

2/3,KWIC/2 (Item 1 from file: 9)
DIALOG(R)File 9:Business & Industry(R)

02236322 (USE FORMAT 7 OR 9 FOR FULLTEXT)
USPS To Use PKI To Offer Electronic Postage
(US Postal **Service moves closer to selling** postage **online after establishing** public- key **infrastructure; service will use PKI as part of Information-Based** Indicia **Program)**
Newsbytes News Network, p N/A
September 10, 1998
DOCUMENT TYPE: Journal ISSN: 0983-1592 (United States)
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 528

(USE FORMAT 7 OR 9 FOR FULLTEXT)
USPS To Use PKI To Offer Electronic Postage
(US Postal **Service moves closer to selling** postage **online after establishing** public- key **infrastructure; service will use PKI as part of Information-Based** Indicia **Program)**

ABSTRACT:
The US **Postal** Service is moving toward selling **postage** online, having set up a **public -key** infrastructure in 8/98. PKI will be used as part of the Information-Based **Indicia** Program (IBIP), which sells **postage** via the Internet, letting users print bar codes on envelopes or labels from printers at...

...the digital stamps consists of a bar code that has unique, scannable data. The US **Postal** Service is losing about $100 mil per year due to **meter** tampering, according to **postal** officials. Meters represent some $21 bil per year in revenues. Cylink Corp (Sunnyvale, CA) provided...

TEXT:
...S.A., 1998 SEP 10 (NB) -- By Merry Mayer, Government Computer News. The U.S. **Postal** Service moved a step closer to selling **postage** online after

it established a **public key** infrastructure last month.

The service will use a PKI as part of the Information-Based **Indicia** Program (IBIP), a program for selling **postage** over the Internet by letting users print bar codes on envelopes or labels from printers...

...stamps has a bar code that provides unique, scannable information. The bar code stores the **postage amount** , user licensing, source and destination **ZIP** codes, along with **date** and time of **postage** printing.

The program will help the **public** buy **postage** more easily, officials said.

The system will also "stem losses from criminal tampering of **postage** meters, counterfeiting of **indicia** and systemic audit and control weaknesses," a **Postal** Service official said.

The service loses about $100 million a year from **meter** tampering, **postal** officials said. Meters account for about $21 billion in revenue a year, **Postal** Service officials said.

The service's PKI will ensure secure transactions for online buyers, IBIP program manager Roy Gordon said. A digital **certificate** establishes the identity of the device; a signature ensures the integrity of the message.

The...

...the Internet Engineering Task Force's X.509 Version 3 digital signature specification, which lets **certificate** authorities read and understand one another, Morbitzer said.

The Cylink PKI system the service will use is designed to produce hundreds of millions of digital certificates, Morbitzer said.

The **Postal** Service plans to issue digital certificates to companies that develop the software and hardware used to sell online **postage** . The companies then sell digital certificates to individuals or companies that want to buy **postage** online, Morbitzer said.

The **Postal** Service sets the standards for the software and hardware, the vendors develop their products, and the service authorizes their use, Gordon said.

Electronic **postage** will initially be targeted to small office and home office users and will eventually be...

...large mailing systems running in mainframe or client-server environments to assist in mail production, **postal** officials said.

The **Postal** Service is beta-testing IBIP services in the Washington area and in Northern Virginia.

It...

...COMPANY NAMES: UNITED STATES **POSTAL** SERVICE
...PRODUCT NAMES: National **postal** service (430000...

2/3,KWIC/3 (Item 1 from file: 810)
DIALOG(R)File 810:Business Wire

0793949 BW0360

SPYRUS: SPYRUS Unveils New Desktop Security for Electronic Postage **Metering**

January 12, 1998

Byline: Business Editors and High-Tech Writers

SPYRUS Unveils New Desktop Security for Electronic Postage **Metering**

...Data Security Conference

Neopost PC Stamp Application Uses the SPYRUS LYNKS Metering Device for Electronic **Postage** Downloading and Envelope Stamp Printing

SAN FRANCISCO--(BUSINESS WIRE)--Jan. 12, 1998--SPYRUS Monday announced that its desktop LYNKS Metering Device (LMD) has been selected for secure electronic **postage** and printing as part of the Neopost PC Stamp electronic **postage meter** system.

These new meters, to be available later in 1998, are part of the United States **Postal** Service (USPS) Information Based **Indicia** Program (IBIP) to replace older mechanical systems with new generation products for directly printing stamps...

...will benefit the small-office home-office (SOHO) and commercial markets through electronic downloading of **postage** and more exacting financial control over **postage** usage.

There are an estimated 10 million SOHO **postage meter** users that will be served by suppliers of this new class of product.

The SPYRUS LYNKS Metering Device is about the **size** of an external modem and connects directly to a standard PC. Driven by an accompanying PC software application, it securely loads and stores **postage value** , and an electronic stamp in the form of a two dimensional bar code is printed...

...the USPS to expedite processing and improve efficiency of mail delivery.

In order to guarantee **postage** integrity, accurate downloading, and to prevent fraud, SPYRUS' **public key** cryptographic technologies are used for digital signature, **certificate** processing and electronic money metering.

The SPYRUS LYNKS Metering Device was developed in close cooperation with Neopost, a leading worldwide manufacturer and distributor of **postage** processing equipment used in metering systems, shipping, and document handling. Neopost will be demonstrating the...

...week. Neopost designed the custom extensions to the IBIP specifications, allowing smooth communications with their **Postage** -on-Call system and their digital scales. PC Stamp, scheduled to enter beta testing later...

...will be marketed by Neopost directly and as part of bundled office software packages.

"The **key** issue in obtaining approval from the USPS for this type of product is security," said...

...3 device and will include active tamper detection and automatic protection of essential values. In **postage meter** applications, these features ensure that the **postal** values stored in the LMD cannot be used fraudulently.

"The LMD's security is contained...

...of businesses to have access to professional mailing capabilities at a fraction of today's **postage meter** costs."

The USPS IBIP will eventually expand to include other classes of users, including high...

...MIME, and Microsoft Authenticode technology. The company's products are used with a variety of **certificate** authority products to

provide critical infrastructure support for issuance and management of a deployed hardware...

2/3,KWIC/4 (Item 1 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

02221072 SUPPLIER NUMBER: 21154848 (USE FORMAT 7 OR 9 FOR FULL TEXT)
USPS To Use PKI To Offer Electronic Postage **09/10/98.**
Newsbytes, n95, pNA
Sept 10, 1998
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 562 LINE COUNT: 00050

USPS To Use PKI To Offer Electronic Postage **09/10/98.**

TEXT:
...S.A., 1998 SEP 10 (NB) -- By Merry Mayer, Government Computer News. The U.S. **Postal** Service moved a step closer to selling **postage** online after it established a **public** -**key** infrastructure last month.
The service will use a PKI as part of the Information-Based **Indicia** Program (IBIP), a program for selling **postage** over the Internet by letting users print bar codes on envelopes or labels from printers...

...stamps has a bar code that provides unique, scannable information. The bar code stores the **postage** **amount** , user licensing, source and destination **ZIP** codes, along with **date** and time of **postage** printing.
The program will help the **public** buy **postage** more easily, officials said.
The system will also "stem losses from criminal tampering of **postage** meters, counterfeiting of **indicia** and systemic audit and control weaknesses," a **Postal** Service official said.
The service loses about $100 million a year from **meter** tampering, **postal** officials said. Meters account for about $21 billion in revenue a year, **Postal** Service officials said.
The service's PKI will ensure secure transactions for online buyers, IBIP program manager Roy Gordon said. A digital **certificate** establishes the identity of the device; a signature ensures the integrity of the message.
The...

...the Internet Engineering Task Force's X.509 Version 3 digital signature specification, which lets **certificate** authorities read and understand one another, Morbitzer said.
The Cylink PKI system the service will use is designed to produce hundreds of millions of digital certificates, Morbitzer said.
The **Postal** Service plans to issue digital certificates to companies that develop the software and hardware used to sell online **postage** . The companies then sell digital certificates to individuals or companies that want to buy **postage** online, Morbitzer said.
The **Postal** Service sets the standards for the software and hardware, the vendors develop their products, and the service authorizes their use, Gordon said.
Electronic **postage** will initially be targeted to small office and home office users and will eventually be...

...large mailing systems running in mainframe or client-server environments to assist in mail production, **postal** officials said.
The **Postal** Service is beta-testing IBIP services in the Washington area and in Northern Virginia.
It...

2/3,KWIC/5 (Item 2 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

02218111 SUPPLIER NUMBER: 21128822 (USE FORMAT 7 OR 9 FOR FULL TEXT)
USPS will use a PKI to manage electronic postage.(public key **infrastructure for** Postal **Service's** Indicia **program) (Government Activity)**
Mayer, Merry
Government Computer News, v17, n29, p14(1)
Sept 7, 1998
ISSN: 0738-4300 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 538 LINE COUNT: 00047

USPS will use a PKI to manage electronic postage.(public key **infrastructure for** Postal **Service's** Indicia **program) (Government Activity)**

TEXT:
The **Postal** Service moved a step closer to selling **postage** online after it established a **public** -**key** infrastructure last month.
The service will use a PKI as part of the Information-Based **Indicia** Program, a program for selling **postage** over the Internet by letting users print bar codes on envelopes or labels from printers...
...stamps has a bar code that provides unique, scannable information. The bar code stores the **postage amount** , user licensing, source and destination **ZIP** codes, along with **date** and time of **postage** printing.
The program will help the **public** buy **postage** more easily, officials said.
The system will also "stem losses from criminal tampering of **postage** meters, counterfeiting of **indicia** and systemic audit and control weaknesses," a **Postal** Service official said.
The service loses about $100 million a year from **meter** tampering, **postal** officials said. Meters account for about $21 billion in revenue a year, **Postal** Service officials said.
The service's PKI will ensure secure transactions for online buyers, IBIP program manager Roy Gordon said. A digital **certificate** establishes the identity of the device; a signature ensures the integrity of the message.
The...

...the Internet Engineering Task Force's X.509 Version 3 digital signature specification, which lets **certificate** authorities read and understand one another, Morbitzer said.
The Cylink PKI system the service will use is designed to produce hundreds of millions of digital certificates, Morbitzer said.
The **Postal** Service plans to issue digital certificates to companies that develop the software and hardware used to sell online **postage** . The companies then sell digital certificates to individuals or companies that want to buy **postage** online, Morbitzer said.
The **Postal** Service sets the standards for the software and hardware, the vendors develop their products, and the service authorizes their use, Gordon said.
Electronic **postage** will initially be targeted to small office and home office users and will eventually be...

...large mailing systems running in mainframe or client-server environments to assist in mail production, **postal** officials said.
The **Postal** Service is beta-testing IBIP services in the Washington area and in Northern Virginia.
It...

...DESCRIPTORS: United States. **Postal** Service...

2/3,KWIC/6 (Item 3 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

02197540 SUPPLIER NUMBER: 20912092 (USE FORMAT 7 OR 9 FOR FULL TEXT)

Stamping Out Fraud.(US Postal Service is creating digital certificates for postage **metering machines) (Government Activity)**
Kerstetter, Jim
PC Week, v15, n28, p14(1)
July 13, 1998
ISSN: 0740-1604 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 402 LINE COUNT: 00035

Stamping Out Fraud.(US Postal **Service is creating digital certificates for** postage **metering machines) (Government Activity)**

TEXT:

Postal Service will use certificates to curb **meter** malfeasance

The U.S. **Postal** Service is dipping a toe into the Internet security pool by applying digital **certificate** technologies to machines instead of users.

The **Postal** Service will announce this week that it is building a PKI (**public -key** infrastructure) for its IBIP (Information Based **Indicia** Program), which is the **Postal** Service's plan to combat more than $100 million in mail fraud by creating digital certificates for **postage** metering machines.

"This project has been in the works for some time now, and what we are concerned about is preventing fraud (in the **Postal** Service's $21 billion **postage** metering channel)," said Nancy Russell, a spokeswoman for IBIP, in Washington.

Although **Postal** Service officials are mum on the subject, there is speculation that IBIP is the first step toward the creation of a long-awaited **Postal** Service-run **certificate** authority.

Talk of such a **certificate** authority, which would place the **Postal** Service in the center of electronic commerce, emerged more than two years ago. But early...

...management team.

For now, Cylink Corp., of Sunnyvale, Calif., has built the PKI for the **Postal** Service's IBIP and will host a pilot project that starts this week in northern Virginia. It will expand to the San Francisco Bay area within a month.

The **Postal** PKI, as it is being called, runs off a SPARC-based server. The **Postal** Service has set up its own space in Cylink's headquarters for attaching certificates to...

...are legitimate machines with legitimate prices, Cylink officials said.

Because of the massive scalability the **Postal** Service will require when it takes the **Postal** PKI project in-house and national early next year, Cylink had to make sure that...

...data field that gives identifying marks and prices that fit the particular needs of the **Postal** Service. The PKI will also interoperate with a variety of algorithms, including elliptic curve, RSA...

...support both Microsoft Corp.'s CryptoAPI and Intel Corp.'s Common Data Security Architecture.

The **Postal** Service's PKI will certify metering machines.

...DESCRIPTORS: United States. **Postal** Service...

...**Public Key** Encryption

2/3,KWIC/7 (Item 1 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)

03951852 Supplier Number: 50295217 (USE FORMAT 7 FOR FULLTEXT)
USPS To Use PKI To Offer Electronic Postage **09/10/98**
Newsbytes, pN/A
Sept 10, 1998

Language: English Record Type: Fulltext
Article Type: Article
Document Type: Newswire; General Trade
Word Count: 536

(USE FORMAT 7 FOR FULLTEXT)
USPS To Use PKI To Offer Electronic Postage **09/10/98**
TEXT:
...S.A., 1998 SEP 10 (NB) -- By Merry Mayer, Government Computer News. The U.S. **Postal** Service moved a step closer to selling **postage** online after it established a **public -key** infrastructure last month.

The service will use a PKI as part of the Information-Based **Indicia** Program (IBIP), a program for selling **postage** over the Internet by letting users print bar codes on envelopes or labels from printers...

...stamps has a bar code that provides unique, scannable information. The bar code stores the **postage amount** , user licensing, source and destination **ZIP** codes, along with **date** and time of **postage** printing.

The program will help the **public** buy **postage** more easily, officials said.

The system will also "stem losses from criminal tampering of **postage** meters, counterfeiting of **indicia** and systemic audit and control weaknesses," a **Postal** Service official said.

The service loses about $100 million a year from **meter** tampering, **postal** officials said. Meters account for about $21 billion in revenue a year, **Postal** Service officials said.

The service's PKI will ensure secure transactions for online buyers, IBIP program manager Roy Gordon said. A digital **certificate** establishes the identity of the device; a signature ensures the integrity of the message.

The...

...the Internet Engineering Task Force's X.509 Version 3 digital signature specification, which lets **certificate** authorities read and understand one another, Morbitzer said.

The Cylink PKI system the service will use is designed to produce hundreds of millions of digital certificates, Morbitzer said.

The **Postal** Service plans to issue digital certificates to companies that develop the software and hardware used to sell online **postage** . The companies then sell digital certificates to individuals or companies that want to buy **postage** online, Morbitzer said.

The **Postal** Service sets the standards for the software and hardware, the vendors develop their products, and the service authorizes their use, Gordon said.

Electronic **postage** will initially be targeted to small office and home office users and will eventually be...

...large mailing systems running in mainframe or client-server environments to assist in mail production, **postal** officials said.

The **Postal** Service is beta-testing IBIP services in the Washington area and in Northern Virginia.

It...

2/3,KWIC/8 (Item 2 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)

03801533 Supplier Number: 48242468 (USE FORMAT 7 FOR FULLTEXT)
HOBBY MARKETS ONLINE AUCTIONS PUT AVID DEALERS, COLLECTORS IN TOUCH WITH EACH OTHER
Information & Interactive Services Report, v19, n2, pN/A
Jan 23, 1998
Language: English Record Type: Fulltext
Document Type: Newsletter; Trade
Word Count: 1463

... note on the bid status of each.

Here's how the online auction works:

* Dealers **register** with the service and list items they will send to the high bidder following a...

...items at a price much lower than their bid prices. "The majority pay a significant **amount** less than their highest bid and they are ecstatic," Dick said. "That's one thing...more than 3,800 lodging properties worldwide. LodgeNet, contact Ann Parker, (605) 988- 1330.

* Secure **Postage** Metering

NetPost Jan. 12 selected the Spyrus desktop Lynks Metering Device (LMD) for secure electronic **postage** and printing as part of the United States **Postal** Services Information Based **Indicia** Program. The program, which will replace older mechanical systems with new-generation processes for directly...

...printers, will benefit small office-home office (SOHO) and commercial markets through electronic download of **postage** . Spyrus estimates the program will serve about 10 million SOHO **postage** **meter** users. The LMDs, which will be available later this year, are about the **size** of an external modem and connect directly to a standard personal computer. To guarantee **postage** integrity, accurate downloading and prevent fraud, Spyrus' **public** **key** cryptographic technologies are used for digital signature, **certificate** processing and electronic money metering. Spyrus is a leading developer of transaction communications devices. Spyrus...

...Solutions Inc. and Dun & Bradstreet Corp. (D&B). Companies can go to either site to **register** their domain names, then obtain a D&B D- U-N-S number. The two...

2/3,KWIC/9 (Item 1 from file: 621)

01597722 Supplier Number: 48218951 (USE FORMAT 7 FOR FULLTEXT)

SPYRUS Unveils New Desktop Security for Electronic Postage **Metering.**

Business Wire, p01120360
Jan 12, 1998
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 897

(USE FORMAT 7 FOR FULLTEXT)

SPYRUS Unveils New Desktop Security for Electronic Postage **Metering.**

TEXT:

...Monday announced that its desktop LYNKS Metering Device (LMD) has been selected for secure electronic **postage** and printing as part of the Neopost PC Stamp electronic **postage** **meter** system.

These new meters, to be available later in 1998, are part of the United States **Postal** Service (USPS) Information Based **Indicia** Program (IBIP) to replace older mechanical systems with new generation products for directly printing stamps...

...will benefit the small-office home-office (SOHO) and commercial markets through electronic downloading of **postage** and more exacting financial control over **postage** usage.

There are an estimated 10 million SOHO **postage** **meter** users that will be served by suppliers of this new class of product.

The SPYRUS LYNKS Metering Device is about the **size** of an external modem and connects directly to a standard PC. Driven by an accompanying PC software application, it securely loads and stores **postage** **value** , and an electronic stamp in the form of a two dimensional bar code is printed...

...the USPS to expedite processing and improve efficiency of mail delivery.

In order to guarantee **postage** integrity, accurate downloading, and to prevent fraud, SPYRUS' **public** **key** cryptographic technologies are

used for digital signature, **certificate** processing and electronic money metering.

The SPYRUS LYNKS Metering Device was developed in close cooperation with Neopost, a leading worldwide manufacturer and distributor of **postage** processing equipment used in metering systems, shipping, and document handling. Neopost will be demonstrating the...

...week. Neopost designed the custom extensions to the IBIP specifications, allowing smooth communications with their **Postage** -on-Call system and their digital scales. PC Stamp, scheduled to enter beta testing later... ...will be marketed by Neopost directly and as part of bundled office software packages.

"The **key** issue in obtaining approval from the USPS for this type of product is security," said...

...3 device and will include active tamper detection and automatic protection of essential values. In **postage** **meter** applications, these features ensure that the **postal** values stored in the LMD cannot be used fraudulently.

"The LMD's security is contained...

...of businesses to have access to professional mailing capabilities at a fraction of today's **postage** **meter** costs."

The USPS IBIP will eventually expand to include other classes of users, including high...

...MIME, and Microsoft Authenticode technology. The company's products are used with a variety of **certificate** authority products to provide critical infrastructure support for issuance and management of a deployed hardware ...

PRODUCT NAMES: 3579514 (**Postage** Meters)

2/3,KWIC/10 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

06120131 Supplier Number: 53735690 (USE FORMAT 7 FOR FULLTEXT)
Stamping Out Crime.(US Postal Service selling stamps over Internet)(Government Activity)
Bruno, Lee
Data Communications, p16(1)
Feb 7, 1999
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 194

(USE FORMAT 7 FOR FULLTEXT)
Stamping Out Crime.(US Postal Service selling stamps over Internet)(Government Activity)
TEXT:
Counterfeiters have been messing with **postal** meters, ripping off the U.S. **Postal** Service (Washington, D.C.) to the tune of $100 million a year. But PKI (**public** **key** infrastructure) technology could help staunch the flow of illicit dollars-and let customers buy **postage** online. The Information Based **Indicia** Program (IBIP) from the U.S. **Postal** Service lets owners of special digital meters download **postage** over the Internet. Its PKI server issues each **meter** a digital **certificate** that authenticates the device, and end-users can then print the **postage** on envelopes in the form of bar codes. Eventually, the **postal** service wants to start downloading **postage** directly to desktop PCs, allowing users to run out the bar codes via networked printers. The PKI for the U.S. **Postal** Service is scalable enough to generate and manage 300 million certificates. Developed by Cylink Corp. (Sunnyvale, Calif.), it's now housed at the vendor's headquarters, but the U.S. **Postal** Service will take charge of it in the next few months. Related 'Net-ready products already are starting to show: Estamp Inc. (Palo Alto, Calif.) is now selling $300 **postage** meters with bundled

digital certificates.
DESCRIPTORS: United States. **Postal** Service
PRODUCT NAMES: 9108381 (**Postal** Services)

2/3,KWIC/11 (Item 2 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

05802940 Supplier Number: 50295217 (USE FORMAT 7 FOR FULLTEXT)
USPS To Use PKI To Offer Electronic Postage **09/10/98**
Newsbytes, pN/A
Sept 10, 1998
Language: English Record Type: Fulltext
Article Type: Article
Document Type: Newswire; General Trade
Word Count: 536

(USE FORMAT 7 FOR FULLTEXT)
USPS To Use PKI To Offer Electronic Postage **09/10/98**
TEXT:
...S.A., 1998 SEP 10 (NB) -- By Merry Mayer, Government Computer News. The U.S. **Postal** Service moved a step closer to selling **postage** online after it established a **public -key** infrastructure last month.

The service will use a PKI as part of the Information-Based **Indicia** Program (IBIP), a program for selling **postage** over the Internet by letting users print bar codes on envelopes or labels from printers...

...stamps has a bar code that provides unique, scannable information. The bar code stores the **postage amount** , user licensing, source and destination **ZIP** codes, along with **date** and time of **postage** printing.

The program will help the **public** buy **postage** more easily, officials said.

The system will also "stem losses from criminal tampering of **postage** meters, counterfeiting of **indicia** and systemic audit and control weaknesses," a **Postal** Service official said.

The service loses about $100 million a year from **meter** tampering, **postal** officials said. Meters account for about $21 billion in revenue a year, **Postal** Service officials said.

The service's PKI will ensure secure transactions for online buyers, IBIP program manager Roy Gordon said. A digital **certificate** establishes the identity of the device; a signature ensures the integrity of the message.

The...

...the Internet Engineering Task Force's X.509 Version 3 digital signature specification, which lets **certificate** authorities read and understand one another, Morbitzer said.

The Cylink PKI system the service will use is designed to produce hundreds of millions of digital certificates, Morbitzer said.

The **Postal** Service plans to issue digital certificates to companies that develop the software and hardware used to sell online **postage** . The companies then sell digital certificates to individuals or companies that want to buy **postage** online, Morbitzer said.

The **Postal** Service sets the standards for the software and hardware, the vendors develop their products, and the service authorizes their use, Gordon said.

Electronic **postage** will initially be targeted to small office and home office users and will eventually be...

...large mailing systems running in mainframe or client-server environments to assist in mail production, **postal** officials said.

The **Postal** Service is beta-testing IBIP services in the Washington area and in Northern Virginia.

It...

2/3,KWIC/12 (Item 3 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

05418087 Supplier Number: 48218951 (USE FORMAT 7 FOR FULLTEXT)
SPYRUS Unveils New Desktop Security for Electronic Postage **Metering.**
Business Wire, p01120360
Jan 12, 1998
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 897

(USE FORMAT 7 FOR FULLTEXT)
SPYRUS Unveils New Desktop Security for Electronic Postage **Metering.**
TEXT:
...Monday announced that its desktop LYNKS Metering Device (LMD) has been selected for secure electronic **postage** and printing as part of the Neopost PC Stamp electronic **postage meter** system.

These new meters, to be available later in 1998, are part of the United States **Postal** Service (USPS) Information Based **Indicia** Program (IBIP) to replace older mechanical systems with new generation products for directly printing stamps...

...will benefit the small-office home-office (SOHO) and commercial markets through electronic downloading of **postage** and more exacting financial control over **postage** usage.

There are an estimated 10 million SOHO **postage meter** users that will be served by suppliers of this new class of product.

The SPYRUS LYNKS Metering Device is about the **size** of an external modem and connects directly to a standard PC. Driven by an accompanying PC software application, it securely loads and stores **postage value** , and an electronic stamp in the form of a two dimensional bar code is printed...

...the USPS to expedite processing and improve efficiency of mail delivery.

In order to guarantee **postage** integrity, accurate downloading, and to prevent fraud, SPYRUS' **public key** cryptographic technologies are used for digital signature, **certificate** processing and electronic money metering.

The SPYRUS LYNKS Metering Device was developed in close cooperation with Neopost, a leading worldwide manufacturer and distributor of **postage** processing equipment used in metering systems, shipping, and document handling. Neopost will be demonstrating the...

...week. Neopost designed the custom extensions to the IBIP specifications, allowing smooth communications with their **Postage** -on-Call system and their digital scales. PC Stamp, scheduled to enter beta testing later...
...will be marketed by Neopost directly and as part of bundled office software packages.

"The **key** issue in obtaining approval from the USPS for this type of product is security," said...

...3 device and will include active tamper detection and automatic protection of essential values. In **postage meter** applications, these features ensure that the **postal** values stored in the LMD cannot be used fraudulently.

"The LMD's security is contained...

...of businesses to have access to professional mailing capabilities at a fraction of today's **postage meter** costs."

The USPS IBIP will eventually expand to include other classes of users, including high...

...MIME, and Microsoft Authenticode technology. The company's products are used with a variety of **certificate** authority products to provide critical infrastructure support for issuance and management of a deployed hardware
...
PRODUCT NAMES: 3579514 (**Postage** Meters)

2/3,KWIC/13 (Item 1 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

10459804 SUPPLIER NUMBER: 21128822 (USE FORMAT 7 OR 9 FOR FULL TEXT)
USPS will use a PKI to manage electronic postage.(public key **infrastructure for** Postal **Service's** Indicia **program) (Government Activity)**
Mayer, Merry
Government Computer News, v17, n29, p14(1)
Sept 7, 1998
ISSN: 0738-4300 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 538 LINE COUNT: 00047

USPS will use a PKI to manage electronic postage.(public key **infrastructure for** Postal **Service's** Indicia **program) (Government Activity)**

TEXT:
The **Postal** Service moved a step closer to selling **postage** online after it established a **public -key** infrastructure last month.
The service will use a PKI as part of the Information-Based **Indicia** Program, a program for selling **postage** over the Internet by letting users print bar codes on envelopes or labels from printers...
...stamps has a bar code that provides unique, scannable information. The bar code stores the **postage amount** , user licensing, source and destination **ZIP** codes, along with **date** and time of **postage** printing.
The program will help the **public** buy **postage** more easily, officials said.
The system will also "stem losses from criminal tampering of **postage** meters, counterfeiting of **indicia** and systemic audit and control weaknesses," a **Postal** Service official said.
The service loses about $100 million a year from **meter** tampering, **postal** officials said. Meters account for about $21 billion in revenue a year, **Postal** Service officials said.
The service's PKI will ensure secure transactions for online buyers, IBIP program manager Roy Gordon said. A digital **certificate** establishes the identity of the device; a signature ensures the integrity of the message.
The...

...the Internet Engineering Task Force's X.509 Version 3 digital signature specification, which lets **certificate** authorities read and understand one another, Morbitzer said.
The Cylink PKI system the service will use is designed to produce hundreds of millions of digital certificates, Morbitzer said.
The **Postal** Service plans to issue digital certificates to companies that develop the software and hardware used to sell online **postage** . The companies then sell digital certificates to individuals or companies that want to buy **postage** online, Morbitzer said.
The **Postal** Service sets the standards for the software and hardware, the vendors develop their products, and the service authorizes their use, Gordon said.
Electronic **postage** will initially be targeted to small office and home office users and will eventually be...

...large mailing systems running in mainframe or client-server environments to assist in mail production, **postal** officials said.
The **Postal** Service is beta-testing IBIP services in the Washington area and in Northern Virginia.
It...

DESCRIPTORS: United States. **Postal** Service...

...**Postal** service

2/3,KWIC/14 (Item 2 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

10322918 SUPPLIER NUMBER: 20912092 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Stamping Out Fraud.(US Postal **Service is creating digital certificates for** postage **metering machines) (Government Activity)**
Kerstetter, Jim
PC Week, v15, n28, p14(1)
July 13, 1998
ISSN: 0740-1604 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 402 LINE COUNT: 00035

Stamping Out Fraud.(US Postal **Service is creating digital certificates for** postage **metering machines) (Government Activity)**

TEXT:

Postal Service will use certificates to curb **meter** malfeasance

The U.S. **Postal** Service is dipping a toe into the Internet security pool by applying digital **certificate** technologies to machines instead of users.

The **Postal** Service will announce this week that it is building a PKI (**public -key** infrastructure) for its IBIP (Information Based **Indicia** Program), which is the **Postal** Service's plan to combat more than $100 million in mail fraud by creating digital certificates for **postage** metering machines.

"This project has been in the works for some time now, and what we are concerned about is preventing fraud (in the **Postal** Service's $21 billion **postage** metering channel)," said Nancy Russell, a spokeswoman for IBIP, in Washington.

Although **Postal** Service officials are mum on the subject, there is speculation that IBIP is the first step toward the creation of a long-awaited **Postal** Service-run **certificate** authority.

Talk of such a **certificate** authority, which would place the **Postal** Service in the center of electronic commerce, emerged more than two years ago. But early...

...management team.

For now, Cylink Corp., of Sunnyvale, Calif., has built the PKI for the **Postal** Service's IBIP and will host a pilot project that starts this week in northern Virginia. It will expand to the San Francisco Bay area within a month.

The **Postal** PKI, as it is being called, runs off a SPARC-based server. The **Postal** Service has set up its own space in Cylink's headquarters for attaching certificates to...

...are legitimate machines with legitimate prices, Cylink officials said.

Because of the massive scalability the **Postal** Service will require when it takes the **Postal** PKI project in-house and national early next year, Cylink had to make sure that...

...data field that gives identifying marks and prices that fit the particular needs of the **Postal** Service. The PKI will also interoperate with a variety of algorithms, including elliptic curve, RSA...

...support both Microsoft Corp.'s CryptoAPI and Intel Corp.'s Common Data Security Architecture.

The **Postal** Service's PKI will certify metering machines.

DESCRIPTORS: United States. **Postal** Service...

...**Postal** service

2/3,KWIC/15 (Item 1 from file: 233)

00501510 98PK07-107

Stamping out fraud -- Postal Service will use certificates to curb meter malfeasance

Kerstetter, Jim

PC WEEK , July 13, 1998 , v15 n28 p14, 1 Page(s)
ISSN: 0740-1604

Stamping out fraud -- Postal Service will use certificates to curb meter malfeasance

Reports that the U.S. **Postal** Service will announce that it is building a **public - key** infrastructure (PKI) for its Information Based **Indicia** Program (IBIP), a plan to create digital certificates for **postage** metering machines. Reports that Cylink Corp. of Sunnyvale, CA, has built the PKI for the **Postal** Service and will host a pilot project in northern Virginia and the San Francisco Bay area. States that Cylink is using X.509 Version 3 certificates for the **Postal** PKI, which will be running off a SPARC-based server. Notes that while **Postal** officials are quiet, there is speculation that the IBIP is the first step toward the creation of a long-awaited **Postal** Service-run **certificate** authority, though notes such plans were discussed once before and set aside. Includes one screen...

Descriptors: **Certificate** Authorities; Federal Government; Security; Shipping/Receiving

?

1/9/2 (Item 1 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

10322918 SUPPLIER NUMBER: 20912092 (THIS IS THE FULL TEXT)
Stamping Out Fraud.(US Postal Service is creating digital certificates for postage metering machines) (Government Activity)
Kerstetter, Jim
PC Week, v15, n28, p14(1)
July 13, 1998
ISSN: 0740-1604 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 402 LINE COUNT: 00035

TEXT:

Postal Service will use certificates to curb **meter** malfeasance

The U.S. **Postal** Service is dipping a toe into the Internet security pool by applying digital **certificate** technologies to machines instead of users.

The **Postal** Service will announce this week that it is building a **PKI** (**public -key** infrastructure) for its **IBIP** (Information Based **Indicia** Program), which is the **Postal** Service's plan to combat more than $100 million in mail fraud by creating digital certificates for postage **metering** machines.

"This project has been in the works for some time now, and what we are concerned about is preventing fraud (in the **Postal** Service's $21 billion postage **metering** channel)," said Nancy Russell, a spokeswoman for **IBIP** , in Washington.

Although **Postal** Service officials are mum on the subject, there is speculation that **IBIP** is the first step toward the creation of a long-awaited **Postal** Service-run **certificate authority** .

Talk of such a **certificate authority** , which would place the **Postal** Service in the center of electronic commerce, emerged more than two years ago. But early plans fizzled because of differing priorities of a new management team.

For now, **Cylink** Corp., of Sunnyvale, Calif., has built the **PKI** for the **Postal** Service's **IBIP** and will host a pilot project that starts this week in northern Virginia. It will expand to the San Francisco Bay area within a month.

The **Postal PKI** , as it is being called, runs off a **SPARC** -based server. The **Postal** Service has set up its own space in **Cylink** 's headquarters for attaching certificates to **metering** machines and authenticating that they are legitimate machines with legitimate prices, **Cylink** officials said.

Because of the massive scalability the **Postal** Service will require when it takes the **Postal PKI** project in-house and national early next year, **Cylink** had to make sure that it can interoperate with a wide variety of security technologies.

Cylink is using X.509 Version 3 certificates and has extended them with an additional data field that gives identifying marks and prices that fit the particular needs of the **Postal** Service. The **PKI** will also interoperate with a variety of algorithms, including **elliptic curve** , RSA and the Digital Signature Algorithm. It will support both Microsoft Corp.'s CryptoAPI and Intel Corp.'s Common Data Security Architecture.

The **Postal** Service's **PKI** will certify **metering** machines.

COMPANY NAMES: **Cylink** Corp.--Product development
INDUSTRY CODES/NAMES: BUSN Any type of business; CMPT Computers and Office Automation
DESCRIPTORS: United States. **Postal** Service--Management; **Postal** service--Metered mail; Computer network equipment industry--Product development
PRODUCT/INDUSTRY NAMES: 3661000 (Telecommunication Systems)
SIC CODES: 3660 Communications Equipment
FILE SEGMENT: CD File 275
?

```
Set     Items   Description
S1          0   AU= (CORDERY R? OR CORDERY, R?)
S2       2987   CERTICOM
S3       1774   ELLIPTIC(2N)CURV? OR HYPERELLIPTIC(2N)CURV?
S4      39581   (PRIVAT? OR PUBLIC? OR SECRET? OR FIRST OR SECOND? OR PRIM-
             AR?)(1W) KEY? ?
S5    1147720   HCC OR AVC OR CODIF? OR DECOD? OR UNENCOD? OR DECRYPT? OR -
             UNENCRYPT? OR UNCRYPT? OR CIPHER? OR CYPHER? OR ENCOD? OR COD-
             E? ? OR CODING? OR ENCOD? OR ENCIPHER? OR ENCYPHER? OR UNCOD?
             OR DECIPHER? OR DECYPHER? OR UNENCIPHER? OR UNENCYPHER?
S6     171600   UNCIPHER? OR UNCYPHER? OR CRYPTO? OR ENCRYPT?
S7     837684   (CERTIFYING? OR CERTIFY OR CERTIFICATION? OR CERTIFIES OR -
             CONFIRM? OR VERIFY? OR ATTEST?)(2N)(STATION? OR AUTHORIT? OR -
             POWER? OR AGENC? OR ORGANI? OR BOARD?) OR CA
S8   14604498   MULTI? OR PLURAL? OR MANY OR SEVERAL? OR NUMER? OR CLUSTER?
              OR GROUP? OR MULTIPL? OR PLENTY? OR CONSIDERABLE? OR TWO OR -
             DUAL OR DOUBL?
S9       1153   S2(S)S3
S10       911   S2(10N)S3
S11        23   S10(S)S7(S)S4
S12         9   RD (unique items)
S13        79   S4(2N)(S5 OR S6)(2N)S7
S14        12   S4(N)(S5 OR S6)(N)S7
S15         9   RD (unique items)
S16         8   S15 AND PY<=1999
S17        56   (S8(2N)S7)(S)S4
S18        30   RD (unique items)
S19        21   S18 AND PY<=1999
S20        21   S19 NOT (S12 OR S16)
? show files
File 275:Gale Group Computer DB(TM) 1983-2002/Aug 15
         (c) 2002 The Gale Group
File 583:Gale Group Globalbase(TM) 1986-2002/Aug 14
         (c) 2002 The Gale Group
File 621:Gale Group New Prod.Annou.(R) 1985-2002/Aug 13
         (c) 2002 The Gale Group
File 636:Gale Group Newsletter DB(TM) 1987-2002/Aug 13
         (c) 2002 The Gale Group
File  16:Gale Group PROMT(R) 1990-2002/Aug 14
         (c) 2002 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 148:Gale Group Trade & Industry DB 1976-2002/Aug 15
         (c)2002 The Gale Group
?
```

12/3,K/1 (Item 1 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2002 The Gale Group. All rts. reserv.

02274462 SUPPLIER NUMBER: 53980307 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Security Solutions. (question and answer).(Column)
Cobb, Michael
e-Business Advisor, 17, 3, 34(1)
March, 1999
DOCUMENT TYPE: Column LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 1743 LINE COUNT: 00146

... is one application of elliptic curve theory and has become a promising new branch of **public - key** cryptography in recent years. This is mainly due to its potential, in some cases, for offering similar security to established **public - key** cryptographic systems, while providing both increased performance and decreased key size. (Elliptic curves are functions...

...as gently looping lines in the X Y plane. Check out this site http://www. **certicom** . **ca** /ecc/weccrypt.htm for white papers and tutorials on **elliptic curves** .) Recent improvements in various aspects of implementation, including the generation of elliptic curves, have made...

12/3,K/2 (Item 1 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)
(c) 2002 The Gale Group. All rts. reserv.

02649170 Supplier Number: 65295189 (USE FORMAT 7 FOR FULLTEXT)
Chrysalis-ITS(R) Goes Wireless, Collaborating with Certicom to Deliver a New Version of Luna(R) CA(3), which Enables Secure Transactions for Wireless Devices.
PR Newswire, p1342
Sept 19, 2000
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 1006

... and Chrysalis-ITS today announced that they have entered into an agreement which delivers an **elliptic curve** -based hardware security module for **Certicom** 's high security wireless **Public Key** Infrastructure (PKI). Certicom's MobileTrust(TM) managed **CA** service (www.certicom.com/mobiletrust), launched today at the Certicom PKS event in San Jose, will include an optimized version of Luna **CA** (3), the industry's most widely used key management system. Luna **CA** (3)-ECC has been enhanced with **Certicom** 's **elliptic curve** cryptography (ECC) protocol, to strengthen the security of **Certicom** 's MobileTrust **CA** service, ensuring best practices for wireless digital certificate issuance.
Under the terms of the agreement...

12/3,K/3 (Item 2 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)
(c) 2002 The Gale Group. All rts. reserv.

02648249 Supplier Number: 65295539 (USE FORMAT 7 FOR FULLTEXT)
Chrysalis-ITS Goes Wireless, Collaborating With Certicom to Deliver a New Version of Luna CA3, Which Enables Secure Transactions for Wireless Devices.
Business Wire, p0196
Sept 19, 2000
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 998

... and Chrysalis-ITS today announced that they have entered into an agreement which delivers an **elliptic curve** -based hardware security module for **Certicom** 's high security wireless **Public Key**

Infrastructure (PKI). Certicom's MobileTrust(TM) managed **CA** service (http://www.chrysalis-its.com/news/partner...

...industry's most widely used key management system. Luna CA3-ECC has been enhanced with **Certicom** 's **elliptic curve** cryptography (ECC) protocol, to strengthen the security of **Certicom** 's MobileTrust **CA** service, ensuring best practices for wireless digital certificate issuance.
Under the terms of the agreement...

12/3,K/4 (Item 3 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)
(c) 2002 The Gale Group. All rts. reserv.

02444609 Supplier Number: 61366763 (USE FORMAT 7 FOR FULLTEXT)
Certicom Reports Third Quarter Results.
PR Newswire, p5304
April 7, 2000
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 1330

... release of a variety of new products for wireless security. WTLS Plus(TM) builds on **Certicom** 's leadership position in developing Internet-standard SSL and **elliptic curve** cryptography (ECC) security technologies to enable wireless e-commerce and secure enterprise connectivity inside any wireless or WAP computing environment. Through the acquisition of Trustpoint of Mountain View, **CA** , Certicom announced its entry into the PKI marketplace. Trustpoint(TM), a comprehensive line of flexible, cross-platform **public key** infrastructure (PKI) products, allows OEMs to develop applications with digital certificate services "built-in." This...

12/3,K/5 (Item 4 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)
(c) 2002 The Gale Group. All rts. reserv.

01569069 Supplier Number: 47969729 (USE FORMAT 7 FOR FULLTEXT)
Wormhole Technologies Licenses Certicom's Security Builder Crypto-Toolkit; Certicom Elliptic Curve Engine Delivers Strong, Fast Cryptography for Security Products.
Business Wire, p9100037
Sept 10, 1997
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 716

... net.com .
Certicom is a leading provider of cryptographic technologies for computing and communications companies. **Certicom** 's core technology is the **Certicom Elliptic Curve** Engine (CE)2 -- a stronger, faster, smaller engine that performs **public - key** encryption and digital signatures required for advanced data security. (CE)2 is available for software...

...development is based in Mississauga, Ontario, Canada, with sales and marketing operations in San Mateo, **CA** . Certicom shares are quoted on the Toronto Stock Exchange under the symbol "CIC." -0-
Note...

12/3,K/6 (Item 5 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)
(c) 2002 The Gale Group. All rts. reserv.

01536768 Supplier Number: 47400882 (USE FORMAT 7 FOR FULLTEXT)
Certicom Elliptic Curve Engine Embedded Within Siemens' Latest Smart Card IC; Joint Development Effort Announced at CardTech/SecurTech '97.
Business Wire, p5210079

May 21, 1997
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 765

... contactless interfaces.
Certicom is a leading provider of cyrptographic technologies for computing and communications companies. **Certicom** 's core technology is the **Certicom Elliptic Curve** Engine (CE)2 -- a stronger, faster, smaller engine that performs **public - key** encyrption and digital signatures required for advanced data security. (CE)2 is available for software...

...headquarters are located in Mississauga, Ontario, Canada, with sales and marketing operations in San Mateo, **CA** , and regional offices in Washington, D.C. and New York. Certicom shares are quoted on...

12/3,K/7 (Item 6 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

01536190 Supplier Number: 47398830 (USE FORMAT 7 FOR FULLTEXT)
Motorola and Certicom demonstrate elliptic curve digital signatures on smart card without crypto coprocessor; Fast, low cost authentication now available.
Business Wire, p05200402
May 20, 1997
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 575

... 28 billion.
Certicom is a leading provider of cryptographic technologies to computing and communications companies. **Certicom** 's core technology is the **Certicom Elliptic Curve** Engine (CE)2 -- a stronger, faster, smaller engine which performs **public - key** encryption and digital signatures required for advanced data security. (CE)2 is available for software...

...headquarters are located in Mississauga, Ontario, Canada, with sales and marketing operations in San Mateo, **CA** , and regional offices in Washington, D.C. and New York. Certicom shares are quoted on...

12/3,K/8 (Item 7 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

01530768 Supplier Number: 47364302 (USE FORMAT 7 FOR FULLTEXT)
Sterling Commerce Licenses Certicom's Elliptic Curve Toolkit for its CONNECT:Conceal Encryption Software.
Business Wire, p05060228
May 6, 1997
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 641

... 300 employees.
Certicom is a leading provider of cryptographic technologies for computing and communications companies. **Certicom** 's core technology is the **Certicom Elliptic Curve** Engine (CE)2 -- a stronger, faster, smaller engine which performs **public - key** encryption and digital signatures required for advanced data security. (CE)2 is available for software...

...headquarters are located in Mississauga, Ontario, Canada, with sales and marketing operations in San Mateo, **CA** , and regional offices in Washington, D.C. and New York. Certicom shares are quoted on...

12/3,K/9 (Item 1 from file: 16)

07060190 Supplier Number: 59450675 (USE FORMAT 7 FOR FULLTEXT)
Internet/Intranets: News Bytes.(Company Business and Marketing)
ENT, v3, n7, p54
April 22, 1998
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Professional
Word Count: 310

... Certicom and Diversinet to Deliver Security for E-Commerce

Certicom Corp. (Mississauga, Ontario, www.certicom. **ca**) and Diversinet Corp. (Toronto, www.dvnet.com) announced that the companies have entered a licensing agreement under which Certicom will provide Diversinet with advanced data security technologies, based on **Certicom** 's **Elliptic Curve** Cryptography (ECC). Diversinet will incorporate ECC into its own **public - key** infrastructure technology product line to provide businesses with security solutions for enterprise networking.

Half of...

?

16/3,K/1 (Item 1 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

02153672 SUPPLIER NUMBER: 20426412
Certificate authorities: who do you trust? (preventing cyberfraud in electronic commerce) (Internet/Web/Online Service Information)
Bruno, Lee
Data Communications, v27, n4, p54(10)
March 21, 1998
ISSN: 0363-6399 LANGUAGE: English RECORD TYPE: Abstract

...ABSTRACT: CA outsourcing services. Building an in-house CA server requires expertise in networking architecture and **public key encryption** . **CA** issues digital certificates to identify users. The certificates are attached to files, E-mail or...

19980321

16/3,K/2 (Item 2 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

02069436 SUPPLIER NUMBER: 19414140 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Electronic commerce. (Technology Information)
Giles, Roosevelt
Network VAR, v5, n5, p26(7)
May, 1997
ISSN: 1082-8818 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 5838 LINE COUNT: 00478

... SSL protocol transparently.
SSL depends on several cryptographic technologies. RSA Data Security's (Redwood City, **CA**) **public key encryption** is used for the exchange of the session key and client-server authentication. Various cryptographic...

19970500

16/3,K/3 (Item 3 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

01666186 SUPPLIER NUMBER: 15055902 (USE FORMAT 7 OR 9 FOR FULL TEXT)
AOCE: a familiar face. (Apple Open Collaboration Environment) (new Apple standard for collaboration)
Snyder, Joel
LAN Magazine, v9, n3, p141(4)
March, 1994
ISSN: 0898-0012 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 2242 LINE COUNT: 00174

... the signature.
The PowerTalk digital signature is based on RSA Data Security's (Redwood City, **CA**) **public - key cryptosystem** algorithms. To get your digital signer (a data tool for creating the signature) , you go...

19940300

16/3,K/4 (Item 1 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

02232231 Supplier Number: 57569798 (USE FORMAT 7 FOR FULLTEXT)
Cyber SIGN Inc. Joins Entrust(R)/Alliance Developer Program.
PR Newswire, p5047

Nov 15, 1999
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 544

... seamless integration of the Cyber-SIGN(R) handwritten signature biometric authentication technology with the Entrust **public - key certification authority , encryption** and digital signature capability. The tightly coupled combination of the Cyber-SIGN biometrics and the ...
19991115

16/3,K/5 (Item 1 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)
(c) 2002 The Gale Group. All rts. reserv.

02334496 Supplier Number: 44561676 (USE FORMAT 7 FOR FULLTEXT)
The Role of The Trusted Third Party
Financial Technology Insight, pN/A
April, 1994
Language: English Record Type: Fulltext
Document Type: Newsletter; Trade
Word Count: 199

(USE FORMAT 7 FOR FULLTEXT)
TEXT:
...parties may act as TTPs for specific functions, the most obvious example here being the **certification authority** for **public encryption keys** . This function is defined under the CCITT recommendations for directory services X.509. This TTP...
19940401

16/3,K/6 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2002 The Gale Group. All rts. reserv.

05110461 Supplier Number: 47802951 (USE FORMAT 7 FOR FULLTEXT)
VISA, MASTERCARD NAME SET ROOT CA
Marlin, Steve
Bank Systems + Technology, p013
July, 1997
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 372

... and SPYRUS' technology is a set of hardware and software components for generating the root **CA** 's **private encryption key** , which will be split into fragments that are each contained on a separate hardware device ...
19970701

16/3,K/7 (Item 1 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2002 The Gale Group. All rts. reserv.

09828401 SUPPLIER NUMBER: 17221249 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Surf's up! The Internet is here. (part 1)(includes related article)
Lawton, George
Telephony, v229, n3, p32(5)
July 17, 1995
ISSN: 0040-2656 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 3086 LINE COUNT: 00247

... secure links between a server and mobile workers on the road. Cylink has incorporated a **public key cryptography certification authority** scheme into this system that allows users to register once in a

central server, and...

19950717

16/3,K/8 (Item 2 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

08200751 SUPPLIER NUMBER: 17609781 (USE FORMAT 7 OR 9 FOR FULL TEXT)
The role of cryptography in network security.
Moore, Mitchell S.
Business Communications Review, v25, n9, p67(6)
Sep, 1995
ISSN: 0162-3885 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 3526 LINE COUNT: 00303

... not only contains the user's public key, but also the authenticated identity of the **CA** .
Public key cryptosystems can also be used to provide an authentication service called "digital signature." Digital signatures permit...

19950900
?

20/3,K/1 (Item 1 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2002 The Gale Group. All rts. reserv.

02275209 SUPPLIER NUMBER: 54022185 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Securing E-commerce Sites.(Internet/Web/Online Service Information)(Tutorial)
Buchner, Mark
MIDRANGE Systems, 12, 3, 28(1)
March 1, 1999
DOCUMENT TYPE: Tutorial ISSN: 1041-8237 LANGUAGE: English
RECORD TYPE: Fulltext
WORD COUNT: 932 LINE COUNT: 00078

... order to issue digital certificates to servers and users within their intranet. CAs broadcast their **public key** and Distinguished Name. People add them as trusted root key to Web servers and browsers. This means your server will trust anyone who has a certificate from that **CA** . There are **several** common CAs in the marketplace. Servers and browsers are shipped with several default trusted root...

19990301

20/3,K/2 (Item 2 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2002 The Gale Group. All rts. reserv.

02245806 SUPPLIER NUMBER: 53250334 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Digital certificates are the key behind electronic commerce.(public key encryption systems)(Technology Information)
Computer Weekly, 36(1)
Nov 12, 1998
ISSN: 0010-4787 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 457 LINE COUNT: 00038

... bona fide.
However, for this procedure to work Internet users must have the details, including **public keys** , of leading certification authorities stored on their PCs. Browsers such as Microsoft's Internet Explorer provide the mechanism for this as they come with the digital certificates of **many** commercial **certification authorities** pre-installed, including the **public keys** .
There are some questionable issues, such as the fact that you have to trust your...

19981112

20/3,K/3 (Item 3 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2002 The Gale Group. All rts. reserv.

02207453 SUPPLIER NUMBER: 20963723 (USE FORMAT 7 OR 9 FOR FULL TEXT)
An introduction to Public Key Infrastructures(network communication) (Technology Information)
Mione, Antonino N.
Digital Systems Report, v20, n2, p20(6)
Summer, 1998
ISSN: 1086-9638 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 2565 LINE COUNT: 00201

... the user's certificate. On the flip side, this means everyone must trust the root **CA** . **Many** people would prefer to pick the CA they trust the most and validate others via...

...makes the root CA a very tempting target for attackers. If the root CA's **private key** is compromised, then an attacker can generate false certificates that look authentic. This organization is...

19980622

20/3,K/4 (Item 4 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2002 The Gale Group. All rts. reserv.

02109489 SUPPLIER NUMBER: 19769766 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Digital certificates and certificate authorities. (public key cryptography) (includes related articles on verifying digital signatures and sending session-key messages) (Government Activity)
Moreh, Jahan
Databased Web Advisor, v15, n9, p73(4)
Sep, 1997
ISSN: 1090-6436 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 2779 LINE COUNT: 00224

... is, what the process for revoking certificates is, and so forth.
Major players in the **CA** business
Many companies are beginning to provide services and/or products related to digital certificates. On the...

...the product side, Entrust Technologies offers a full set of products in the area of **Public Key** Infrastructure (PKI) and digital certificates. Other noteworthy vendors are the U.S. Post Office, General...

19970900

20/3,K/5 (Item 5 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2002 The Gale Group. All rts. reserv.

02067045 SUPPLIER NUMBER: 19437310 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Fortifying your server for secure transactions.(Site Building) (Internet/Web/Online Service Information)(Column)(Tutorial)
Krick, John
Computer Shopper, v17, n6, p628(2)
June, 1997
DOCUMENT TYPE: Column Tutorial ISSN: 0886-0556 LANGUAGE: English
RECORD TYPE: Fulltext; Abstract
WORD COUNT: 1894 LINE COUNT: 00149

... certificates verify to both parties in a transaction that the holder of a public or **private key** is the person or organization they claim to be. The key user's identity is attested to by a trusted third party, the **Certification Authority** .
Many vendors are jumping into the new industry of certification technology, including GTE with its CyberTrust...

19970600

20/3,K/6 (Item 6 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2002 The Gale Group. All rts. reserv.

02000717 SUPPLIER NUMBER: 18768621 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Protecting your data with cryptography. (Technology Information)
Foroozesh, Mehrdad
UNIX Review, v14, n12, p55(6)
Nov, 1996
ISSN: 0742-3136 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 4013 LINE COUNT: 00329

... in several commercial products.
Over the years, disputes have arisen over licenses and patents for **public - key** cryptosystems. To address some of these issues, several

companies formed a consortium known as the **Public Key** Partners (PKP; Sunnvale, **CA**). This **group** now holds the patents and exclusive licensing rights to all **public - key** cryptosystems on behalf of MIT, Stanford University RSA Data Security, and others.(9)
The mathematical...

19961100

20/3,K/7 (Item 7 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

01886563 SUPPLIER NUMBER: 17963356 (USE FORMAT 7 OR 9 FOR FULL TEXT)
New tools for collaboration emerge in the public network. (groupware applications)(includes related article on Internet groupware security) (Company Business and Marketing)(Cover Story)
Cummings, Joanne
Telecommunications, v29, n12, p25(3)
Dec, 1995
DOCUMENT TYPE: Cover Story ISSN: 0278-4831 LANGUAGE: English
RECORD TYPE: Fulltext; Abstract
WORD COUNT: 2262 LINE COUNT: 00178

... nobody's really interesed in the Internet as an infrastructure," she says. CommerceNet currently runs **two certification authorities** that issue **public key** certificates to its members, which enables them to experiment with the security technology. The group...

19951200

20/3,K/8 (Item 1 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

02182252 Supplier Number: 55863724 (USE FORMAT 7 FOR FULLTEXT)
CitX Through Baltimore Technologies to Build Secure Certification Authority (CA) for Management and Authentication of Digital Identities.
PR Newswire, p3453
Sept 27, 1999
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 846

... and services for a wide range of e-Commerce and enterprise applications. Its products include **Public Key** Infrastructure (PKI) systems, cryptographic toolkits, security applications and hardware cryptographic devices. Baltimore UniCERT is a modular, scalable, **multipurpose** Certificate Authority (**CA**) which issues and manages digital certificates for a wide range of applications including e-mail...
19990927

20/3,K/9 (Item 2 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

01791469 Supplier Number: 53594691 (USE FORMAT 7 FOR FULLTEXT)
Digital Signature Trust Company Validates Concept of Industry-Wide Certificate Authority in Securities Industry Pilot.
PR Newswire, p6754
Jan 19, 1999
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 867

... root CA for the pilot. As a part of ABAecom's offer, DST provided the **public key** infrastructure (PKI) behind the root CA for SIRCA. DST

also collaborated with the National Association...

...signing process with the respective PKI technologies used by the firms. Additionally, DST provided the **CA** operation for **two** of the participating firms.
"As our world becomes increasingly electronic, the necessity to facilitate secure...
19990119

20/3,K/10 (Item 3 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

01790427 Supplier Number: 53585671 (USE FORMAT 7 FOR FULLTEXT)
Entrust Technologies Accelerates Public-Key Infrastructure Evolution with Release of Open Toolkits to Developer Community.
Business Wire, p0174
Jan 18, 1999
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 896

... RSA Data Security Conference -- Entrust(R) Technologies Inc. (Nasdaq: ENTU), the global leader in managed **public - key** infrastructures (PKI), today announced that its open development toolkits are now available for download from...

...in the PKI industry, Entrust Technologies is providing toolkits for building applications that work with **multiple** PKI and **Certification Authority** (CA) products or services from vendors such as Entrust, Baltimore Technologies, Microsoft, Netscape, VeriSign and...
19990118

20/3,K/11 (Item 4 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

01576983 Supplier Number: 48029654 (USE FORMAT 7 FOR FULLTEXT)
Entrust Technologies' Announces Solution for Secure Internet Banking and Brokerage.
Business Wire, p10061271
Oct 6, 1997
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 752

... of its Scotia OnLine service and has quickly become a leader in the issuance of **public - key** certificates from its **two** Entrust-based **Certification Authorities** .
Entrust/Direct is based on sound and proven cryptography, and allows customer to control their...
19971006

20/3,K/12 (Item 5 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

01553533 Supplier Number: 47857915 (USE FORMAT 7 FOR FULLTEXT)
TIS Ships "Total Solution" For User Controlled Encryption Key Recovery.
Business Wire, p7251232
July 25, 1997
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 990

... both unnecessary and ill-advised to link use of key recovery with a

government-mandated **public key** infrastructure for electronic commerce. For this reason, TIS does not support provisions in proposed U.S. legislation that would force top-down linkages between key recovery and issuance of **public - key** certificates by "Government-approved" **certification authorities** .

"Combining **two** complex and fast moving sets of technologies like key recovery and **public - key** infrastructures creates unnecessary complications and delays for users. Forcing such a link is a bad...

...means users can choose -- and change -- which forms of key management and which types of **public - key** certificates they want to use."

RECOVERKEY COMPONENTS

The RecoverKey Key Recovery Center (KRC) provides for...

19970725

20/3,K/13 (Item 1 from file: 636)

DIALOG(R)File 636:Gale Group Newsletter DB(TM)

03872268 Supplier Number: 48452811 (USE FORMAT 7 FOR FULLTEXT)

-SPYRUS: SPYRUS and DataCard team to develop public key smart card personalization solutions

M2 Presswire, pN/A

April 29, 1998

Language: English Record Type: Fulltext

Document Type: Newswire; Trade

Word Count: 756

... transactions using the smart card. In the future, the personalization system is designed to support **multiple certification authorities** and smart cards. "Over the next few years, we believe that enterprises across the globe will be deploying **public key** infrastructures to support a wide variety of on-line activities," according to John Doyle, vice...

19980429

20/3,K/14 (Item 2 from file: 636)

DIALOG(R)File 636:Gale Group Newsletter DB(TM)

03477571 Supplier Number: 47170430 (USE FORMAT 7 FOR FULLTEXT)

Certificate Authorities: To Outsource Or Not?

Bank Technology News, pN/A

March 1, 1997

Language: English Record Type: Fulltext

Document Type: Magazine/Journal; Trade

Word Count: 2226

... a trusted third party between senders and recipients of electronic correspondence, ensuring the identity of **public key** owners. In addition, individuals misrepresenting themselves to the USPS is a criminal activity for which...

...be prosecuted. There's also a psychological benefit to using the Postal Service as the **CA** . **Many** consumers will believe that if the Postal Service says it's okay to do transactions...

19970301

20/3,K/15 (Item 3 from file: 636)

DIALOG(R)File 636:Gale Group Newsletter DB(TM)

01479941 Supplier Number: 42048180 (USE FORMAT 7 FOR FULLTEXT)

VENDORS CHOOSE RSA ENCRYPTION TECHNOLOGY AS A STANDARD:

Technical Computing, v6, n6, pN/A

May, 1991

Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 143

(USE FORMAT 7 FOR FULLTEXT)
TEXT:
...unable to decide a new deadline, six major computer vendors are preparing to endorse a **public - key** encryption system developed by RSA Data Security Inc. (Redwood City, **CA**). The **group** includes Novell, Inc., Lotus, and DEC, which have already signed licenses with RSA. Sun Microsystems...
19910501

20/3,K/16 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

07044859 Supplier Number: 57769191 (USE FORMAT 7 FOR FULLTEXT)
Knock, knock ... who's there?(public key encryption)(Technology Information)
Rothman, Mike
Communications News, v36, n6, p28
June, 1999
Language: English Record Type: Fulltext Abstract
Document Type: Magazine/Journal; Trade
Word Count: 1442

... in a secure business transaction
1 A trusted third party known as a certificate authority (**CA**) issues **two** keys: a **private key** to an individual and a **public key** validated by the CA accessible to the general public. The CA can be internal to...
19990601

20/3,K/17 (Item 2 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

06088335 Supplier Number: 53614962 (USE FORMAT 7 FOR FULLTEXT)
Digital Certificates Catch On with Securities Firms.
American Banker, v164, n13, pNA
Jan 21, 1999
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 763

... signed the certificate requests coming from the participating firms and demonstrated interoperability among the various **public key** infrastructure vendors. DST was also the **CA** servicer for **two** of the brokerages and provided the registration of certificates in collaboration with the National Association...
19990121

20/3,K/18 (Item 3 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

06058765 Supplier Number: 54841573 (USE FORMAT 7 FOR FULLTEXT)
LAN-to-LAN VPNs: Secure Enough?(virtual private network)(Technology Information)
Steinke, Steve
Network, pNA
August 1, 1998
Language: English Record Type: Fulltext Abstract
Document Type: Magazine/Journal; Trade
Word Count: 4249

... this writing, Axent does not offer a hardware-assisted encryption product.
Network Associates (Santa Clara, **CA**) acquired **several** security vendors in 1998, including Trusted Information Systems, which produces the Gauntlet Firewall. The Gauntlet...

...VPN comes with its own certificate authority, letting an organization generate and verify X.509 **public key** certificates.
Somewhat surprisingly for a security product, Gauntlet Global VPN runs on Windows 95. The...
19980801

20/3,K/19 (Item 4 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2002 The Gale Group. All rts. reserv.

05811921 Supplier Number: 50317382 (USE FORMAT 7 FOR FULLTEXT)
PKI tames network security
McClure, Stuart
InfoWorld, v20, n37, p65
Sept 14, 1998
Language: English Record Type: Fulltext
Article Type: Article
Document Type: Magazine/Journal; Trade
Word Count: 2279

... Directory Access Protocol (LDAP) responds to requests to deliver the stored public key certificates.
The **CA** generates **two** separate pairs of public and **private keys** for each user or server. One pair is used for encrypting and decrypting information, and...

...this common problem: nonrepudiation. Nonrepudiation is the electronic equivalent of a signed log. Because the **CA** maintains **two** key pairs, the recipient of a digital signature, which was created with the sender's **private key** , can compare it to the signature generated by the receiver with the sender's **public key** . Thus, the recipient can confirm that the encrypted stream or file was actually made by...
19980914

20/3,K/20 (Item 5 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2002 The Gale Group. All rts. reserv.

04097718 Supplier Number: 45971490
Groupware Over the Internet? Well, Not Yet
Telecommunications, v29, n12, p26
Dec, 1995
Language: English Record Type: Abstract
Document Type: Magazine/Journal; Trade

ABSTRACT:
...CommerceNet executive director Cathy Medlich. The Internet goes almost everywhere at little cost. CommerceNet runs **two certification authorities** that issue **public key** certificates to members so that they can experiment with security technology. It is running several...
19951201

20/3,K/21 (Item 1 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2002 The Gale Group. All rts. reserv.

09410709 SUPPLIER NUMBER: 19261442 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Electronic notaries can provide safe transmission. (The View from Inside) (Technology Information)(Column)

Houser, Walter R.
Government Computer News, v16, n7, p34(1)
March 17, 1997
DOCUMENT TYPE: Column ISSN: 0738-4300 LANGUAGE: English
RECORD TYPE: Fulltext; Abstract
WORD COUNT: 811 LINE COUNT: 00068

... CommerceNet of Palo Alto, Calif.

An enterprising digital notary may need to sign up with **several certifying authorities** because their solutions and methods may be incompatible, based on differing **public / private - key** algorithms.

One gets a secret private key and a public key to be widely distributed...

19970317
?

et	Items	Description
S1	0	AU= (CORDERY R? OR CORDERY, R?)
S2	704	CERTICOM
S3	641	ELLIPTIC(2N)CURV? OR HYPERELLIPTIC(2N)CURV?
S4	15704	(PRIVAT? OR PUBLIC? OR SECRET? OR FIRST OR SECOND? OR PRIMAR?)(1W) KEY? ?
S5	582518	HCC OR AVC OR CODIF? OR DECOD? OR UNENCOD? OR DECRYPT? OR UNENCRYPT? OR UNCRYPT? OR CIPHER? OR CYPHER? OR ENCOD? OR CODE? ? OR CODING? OR ENCOD? OR ENCIPHER? OR ENCYPHER? OR UNCOD? OR DECIPHER? OR DECYPHER? OR UNENCIPHER? OR UNENCYPHER?
S6	65620	UNCIPHER? OR UNCYPHER? OR CRYPTO? OR ENCRYPT?
S7	281475	(CERTIFYING? OR CERTIFY OR CERTIFICATION? OR CERTIFIES OR CONFIRM? OR VERIFY? OR ATTEST?)(2N)(STATION? OR AUTHORIT? OR POWER? OR AGENC? OR ORGANI? OR BOARD?) OR CA
S8	6422123	MULTI? OR PLURAL? OR MANY OR SEVERAL? OR NUMER? OR CLUSTER? OR GROUP? OR MULTIPL? OR PLENTY? OR CONSIDERABLE? OR TWO OR DUAL OR DOUBL?
S9	266	S2(S)S3
S10	7	S9(S)S7
S11	5	RD (unique items)
S12	339	S4(S)(S5 OR S6)(S)S7
S13	239	S4(10N)(S5 OR S6)(10N)S7
S14	125	S4(5N)(S5 OR S6)(5N)S7
S15	43	S4(2N)(S5 OR S6)(2N)S7
S16	32	S15 AND PY<=1999
S17	28	RD (unique items)
S18	23	(S8(2N)S7)(S)S4
S19	17	RD (unique items)
S20	13	S19 AND PY<=1999
S21	13	S20 NOT S17

YSTEM:OS - DIALOG OneSearch
File 15:ABI/Inform(R) 1971-2002/Aug 14
(c) 2002 ProQuest Info&Learning
***File 15: Alert feature enhanced for multiple files, duplicate**
removal, customized scheduling. See HELP ALERT.
File 810:Business Wire 1986-1999/Feb 28
(c) 1999 Business Wire
File 647:CMP Computer Fulltext 1988-2002/Aug W3
(c) 2002 CMP Media, LLC
File 674:Computer News Fulltext 1989-2002/Aug W2
(c) 2002 IDG Communications
File 696:DIALOG Telecom. Newsletters 1995-2002/Aug 14
(c) 2002 The Dialog Corp.
File 98:General Sci Abs/Full-Text 1984-2002/Jun
(c) 2002 The HW Wilson Co.
File 624:McGraw-Hill Publications 1985-2002/Aug 14
(c) 2002 McGraw-Hill Co. Inc
File 369:New Scientist 1994-2002/Jul W2
(c) 2002 Reed Business Information Ltd.
File 484:Periodical Abs Plustext 1986-2002/Aug W2
(c) 2002 ProQuest
***File 484: SELECT IMAGE AVAILABILITY FOR PROQUEST FILES**
ENTER 'HELP PROQUEST' FOR MORE
File 813:PR Newswire 1987-1999/Apr 30
(c) 1999 PR Newswire Association Inc
File 370:Science 1996-1999/Jul W3
(c) 1999 AAAS
***File 370: This file is closed (no updates). Use File 47 for more current**
information.
File 553:Wilson Bus. Abs. FullText 1982-2002/May
(c) 2002 The HW Wilson Co
File 95:TEME-Technology & Management 1989-2002/Aug W2
(c) 2002 FIZ TECHNIK

11/3,K/1 (Item 1 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext

01223527 CMP ACCESSION NUMBER: INW20000925S0022
Security Goes Wireless
RUTRELL YASIN
INTERNETWEEK, 2000, n 830, PG13
PUBLICATION DATE: 000925
JOURNAL CODE: INW LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: NEWS & ANALYSIS
WORD COUNT: 371

... signatures legally binding. The new law is expected to stimulate all e-commerce, including wireless.

Certicom launched the first Certificate Authority (**CA**), dubbed MobileTrust, that will issue digital certificates to users of handheld and wireless devices supporting **Elliptic Curve** Cryptography encryption.

ECC is an encryption method suited for resource-constrained devices such as cellular...

11/3,K/2 (Item 2 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext

01145259 CMP ACCESSION NUMBER: EET19971117S0014
Code breakers lured for crypto challenge (Late News)
ELECTRONIC ENGINEERING TIMES, 1997, n 981, PG08
PUBLICATION DATE: 971117
JOURNAL CODE: EET LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: News
WORD COUNT: 188

TEXT:
... certain public-key communities, primarily around RSA and PGP algorithms, will spur interest in the **elliptic curve** class of public-key crypto algorithms. The company has launched an **Elliptic Curve** Cryptosystem challenge (www. **certicom** . **ca**), and is offering prizes for determining an ECC private key based on knowledge of the...

11/3,K/3 (Item 1 from file: 696)
DIALOG(R)File 696:DIALOG Telecom. Newsletters

00745263
THE BUSINESS OF DIGITAL SIGNATURES
Electronic Commerce News
October 2, 2000 VOL: 5 ISSUE: 39 DOCUMENT TYPE: NEWSLETTER
PUBLISHER: PHILLIPS BUSINESS INFORMATION
LANGUAGE: ENGLISH WORD COUNT: 798 RECORD TYPE: FULLTEXT

TEXT:
An Interview With **Certicom** Vice President Of Field Operations Richard Depew

Certicom [CERT], a Hayward, Calif.-based encryption technology firm, opened a certificate authority service center Oct...

...into effect (see
ECN 9/25/00). In this special two-part series, Richard Depew, **Certicom** 's

vice
president of field operations, tells ECN how the business of authentication relates to...
...world
and, as such, we do have to be in a large range of industries. **Certicom** has
taken the approach of focusing on the markets that are most applicable for our...

...and are announcing a
wireless extension to their product strategy, which brings them back to **Certicom** .

ECN: What role do your partnerships with companies like AT&T [T], Motorola [MOT], and...

...OEM [original equipment manufacturer]
[clients] are those who will need certificates as part of their **Certicom** -enabled
security solution. We do not have to rely on a less vertically integrated security...

...of differences. The device is typically much
more constrained than a desktop or server. When **Certicom** launched SSL [Secure
Socket Layer] Plus for Embedded Systems, we built the product from the...

...limited processing power, the algorithms have
to be much more efficient. This is why ECC [**elliptic curve** cryptosystems] has
been successful in the wireless environment and is becoming important in smart
card...world as there are many more points of attack compared to the wireline
world. With **Certicom** mutual authentication, using both server and client
certificates and ECDSA [**Elliptic Curve** Digital Signature Algorithm] for digital
signatures (in accordance with the new E-Sign law) ... we...

...devices.

ECN: What companies do you view as your prime competition? Where do you view **Certicom** vis-a-vis these competitors?
Depew: Nobody has the same comprehensive solution set that we do, so it depends on the product. **Certicom** will be the first company to offer ECC certificates for the wireless environment for both servers and clients. Other
companies in the **CA** [certificate authority] business, whether product or services, include VeriSign Inc. [VRSG], Baltimore Technologies plc [BALT...

...to these companies. In the crypto[ography] space, RSA
Security Inc. [RSAS] continues to be **Certicom** 's biggest competitor.
Certicom will soon offer RSA technology in its products in the United States, due to the patent expiring, rounding out our offering. **Certicom** is
positioned versus RSA based on our ownership of the ECC marketplace and expertise in...

...Baltimore Technologies plc] we do not run into those kits in the field very
often. **Certicom** entered the handheld VPN [virtual private network] space because
there was a strong market need, and no competitors providing a solution that can
interoperate with multiple gateways.
(For Richard Depew, **Certicom** , Lorraine Kauffman, 510/780-5417.)
...

11/3,K/4 (Item 2 from file: 696)
DIALOG(R)File 696:DIALOG Telecom. Newsletters

00616592
Government, Industry Collaborate On First Pilot In North America Combining SET, Smart Cards
Report on Electronic Commerce
July 28,1998 VOL: 5 ISSUE: 14 DOCUMENT TYPE: NEWSLETTER
PUBLISHER: BRP PUBLICATIONS
LANGUAGE: ENGLISH WORD COUNT: 897 RECORD TYPE: FULLTEXT

TEXT:
...Officials with Certicom Corp., developer of the **elliptic curve** technology, said ECC and smart cards can provide greater speed, security performance improvements, cost savings...

...to enable an interoperable, efficient system from the smart card, to the server, to the **CA** [certificate authority] underscores the industry's enthusiasm for **elliptic curve** technology and its demand for increased efficiency for online financial transactions," said Philip Deck, president and chief executive officer for **Certicom** .

11/3,K/5 (Item 3 from file: 696)
DIALOG(R)File 696:DIALOG Telecom. Newsletters

00053532
Items of Interest
Report on Smart Cards
June 17,1996 VOL: 10 ISSUE: 12 DOCUMENT TYPE: NEWSLETTER
PUBLISHER: BRP PUBLICATIONS
LANGUAGE: ENGLISH WORD COUNT: 1039 RECORD TYPE: FULLTEXT

TEXT:
...Toronto-based **Certicom** Corp. has opened an office in California to better position the company to license its **elliptic curve** cryptosystem (ECC) public key technology to original equipment manufacturers in the United States. The office...

...strategic partnerships, combined with key technical knowledge of the security market, is sure to broaden **Certicom** 's relationships in the United States," said Gary Hughes, president and chief executive officer of **Certicom** . The company also announced the appointment of Bruce MacInnis to the post of chief financial officer. **Certicom** : Contact Jennifer Vancini, 200 Matheson Blvd. West, Suite 103, Mississauga, Ontario L5R 3L7, Canada. Phone: +1 905-507-4220. E-mail: jvancini@ **certicom** . **ca** .

*

?

17/3,K/1 (Item 1 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

02277107 86921891
Making e-mail secure
Shirley Daniels
Work Study v46n6 PP: 207-214 1997
ISSN: 0043-8022 JRNL CODE: WST
WORD COUNT: 5352

...TEXT: be made with a standard password/phrase (which may be null) and that keyring serially **encrypted** in the **public keys** of the **organization** 's **certification** keys. Should the user lose access to their private key(s), they would then be...

17/3,K/2 (Item 2 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01903660 05-54652
Signed, sealed, and delivered: A ritual for digital business
Wright, Benjamin
Commercial Law Bulletin v14n3 PP: 10-13 May/Jun 1999
ISSN: 0888-8000 JRNL CODE: CLL
WORD COUNT: 1882

...TEXT: they fall short. They are too abstract. They have no flourish, no flair, no style.

Public key cryptography , when supported by a **certification authority** , is known as **public key** infrastructure (PKI). The best-known provider of PKI is Verisign, http://www.verisign.com. Don...

17/3,K/3 (Item 3 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01772409 04-23400
Serious about security? Who the X.509 are you?
Gibbs, Mark
Network World v16n5 PP: 34 Feb 1, 1999
ISSN: 0887-7661 JRNL CODE: NWW
WORD COUNT: 637

...TEXT: message digest," a value that describes the contents of the fields.This digest is then **encrypted** with the **certification authority** 's **private key** to create the signature value.

That's what X.509 is - a specification of the...

17/3,K/4 (Item 4 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01685350 03-36340
Public-key certificates protect corporate jewels
Stallings, William
Network World v15n33 PP: 29 Aug 17, 1998
ISSN: 0887-7661 JRNL CODE: NWW
WORD COUNT: 751

...TEXT: all practical purposes, two different certificates will yield two different hash codes.

Next the CA **encrypts** the hash **code** with the **CA** 's **private key** to

produce the signature. A common public-key algorithm for this purpose comes from RSA...

17/3,K/5 (Item 5 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01605993 02-56982
Digital signatures and their use in treasury
Tinucci, Joseph D
TMA Journal v18n2 PP: 39-42 Mar/Apr 1998
ISSN: 1080-1162 JRNL CODE: JCG
WORD COUNT: 2151

...TEXT: the CA's own certificates, information encrypted with their private key (which the viewer would **decrypt** with the **CA** 's **public key** to authenticate the **CA**), date and time stamps, disclaimers, and other material. The receiver of the message that includes...

17/3,K/6 (Item 6 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01385364 00-36351
Securing the Web
Baker, Steven
UNIX Review v15n3 PP: 23-31 Mar 1997
ISSN: 0742-3136 JRNL CODE: UXR
WORD COUNT: 2681

...ABSTRACT: and normal requests and handle the initial negotiation phase. Web security schemes that depend on **public** - **key** **cryptography** require a **Certification** **Authority** to vouch for the credentials and provide the public keys needed for secure Web servers...
...TEXT: joint proposal by MasterCard and Visa. A Central Aumoriy

Web security schemes that depend on **public** - **key** **cryptography** require a **Certification** **Authority** (**CA**) to vouch for the credentials (authenticate) and provide the public keys needed for secure Web...

17/3,K/7 (Item 7 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01380695 00-31682
Keeping secrets: Data security in the e-mail
Cohen, Georgina
Australian Accountant v67n1 PP: 34-36 Feb 1997
ISSN: 0004-8631 JRNL CODE: AAA
WORD COUNT: 1360

...TEXT: Rivest, Adi Shamir, and Leonard Adleman), will be used in conjunction with 'trusted third party' **certification** **authorities** .

Public **key** **encryption** uses asymmetric keys. One key is used to encrypt a message, and a different key...

17/3,K/8 (Item 8 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01064729 97-14123
Surf's up! The Internet is here (deal with it) - Part 1
Lawton, George
Telephony v229n3 PP: 32-36 Jul 17, 1995

ISSN: 0040-2656 JRNL CODE: TPH
WORD COUNT: 3252

...TEXT: secure links between a server and mobile workers on the road. Cylink has incorporated a **public key cryptography certification authority** scheme into this system that allows users to register once in a central server, and...

17/3,K/9 (Item 9 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01043829 96-93222
Spyglass' Parker: 'Net security critical
Parsons, Michael; Booker, Ellis
Computerworld v29n22 PP: 54 May 29, 1995
ISSN: 0010-4841 JRNL CODE: COW
WORD COUNT: 614

...ABSTRACT: Spyglass Inc., discusses commerce and security on the World-Wide Web. Parker thinks that a **certification authority** in charge of **public - key encryption** is the solution to offering secure commerce on the World-Wide Web.
...TEXT: What will enable secure commerce on the World-Wide Web?

A You must have a **certification authority** if you are using a **public - key encryption** . The **certification authority** provides a way for a third party to establish that the buyer and the seller...

17/3,K/10 (Item 10 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

00649940 92-64880
COSINE Sub-Project P8: Security Services
Purser, Michael
Computer Networks & ISDN Systems v25n4,5 PP: 476-482 Nov 1992
ISSN: 0376-5075 JRNL CODE: CNI

...ABSTRACT: limited but attainable goals of secure electronic mail and secure remote access, supported by a **certification authority** and **public key cryptographic** functions, are intended to demonstrate that these functions can be provided in a relatively short...

17/3,K/11 (Item 1 from file: 810)
DIALOG(R)File 810:Business Wire

0946866 BW1405

CHRYSALIS: Chrysalis-ITS Announces Availability of Entrust-Ready Luna CA3

December 02, 1998

Byline: Business Editors

...including Solaris and Windows NT. Luna CA3 toolkits are available an d
include the PKCS 11 **public key cryptography** standard. Luna **CA** , with FIPS 140-1 Level 2 configuration, is also Entrust-Ready and pricing starts at...

17/3,K/12 (Item 2 from file: 810)
DIALOG(R)File 810:Business Wire

0941337 BW1132

ENTRUST: Entrust/CommerceCA 4.1 Delivers Advanced Certification Authority (CA) Solution for SET

November 18, 1998

Byline: Business Editors

...dedicated to ensuring the privacy and
authenticity of data communications enterprise-wide. Its award-winning
public - key infrastructure technology combines **certification authority** ,
encryption and digital signature capabilities with fully automated key
management. Widely used by financial institutions, government...

17/3,K/13 (Item 3 from file: 810)
DIALOG(R)File 810:Business Wire
(c) 1999 Business Wire . All rts. reserv.

0924228 BW0244

HEWLETT PACKARD 3: New Internet VAR and ISP Alliances Strengthen HP Covision Presence Across the United States

October 19, 1998

Byline: Computer Writers

...single sign-on, Virtual Private Networks,
Internet and extranet security and Raptor firewalls;
-- Entrust Technologies -- **public - key** infrastructure technology that
combines **certification authority** , **encryption** and
digital-signature capabilities with fully automated key
management;
-- Internet Security Systems, Inc. -- adaptive network...

17/3,K/14 (Item 4 from file: 810)
DIALOG(R)File 810:Business Wire
(c) 1999 Business Wire . All rts. reserv.

0870141 BW1180

ENTRUST: RE: Entrust Technologies Announces Fully Integrated Suite of Products to Secure the Desktop

June 23, 1998

Byline: Business Editors

...dedicated to ensuring the privacy and
authenticity of data communications enterprise-wide. Its
award-winning **public - key** infrastructure technology combines
certification authority , **encryption** and digital signature
capabilities with fully automated key management. Used by financial
institutions, government agencies...

17/3,K/15 (Item 5 from file: 810)
DIALOG(R)File 810:Business Wire
(c) 1999 Business Wire . All rts. reserv.

0870132 BW1172

ENTRUST: RE: Entrust Technologies Announces One-Source Way to Issue Digital Certificates for the Web, VPNs, and for SET Financial Transactions

June 23, 1998

Byline: Business Editors

...dedicated to ensuring the privacy and authenticity of data communications enterprise-wide. Its award-winning **public - key** infrastructure technology combines **certification authority** , **encryption** and digital signature capabilities with fully automated key management. Used by financial institutions, government agencies...

17/3,K/16 (Item 6 from file: 810)
DIALOG(R)File 810:Business Wire

0869393 BW0125

ENTRUST TECHNOLOGIES: Fifteen Announcements Highlight New Entrust Technologies' Relationships; Entrust-Ready Products Unveiled at Entrust SecureSummit '98

June 22, 1998

Byline: Business Editors & Computer Writers

...dedicated to ensuring the privacy and authenticity of data communications enterprise-wide. Its award-winning **public - key** infrastructure technology combines **certification authority** , **encryption** and digital signature capabilities with fully automated key management. Used by financial institutions, government agencies...

17/3,K/17 (Item 1 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext

01194116 CMP ACCESSION NUMBER: WIN19990615S0010
Super Security - Here's how to protect your valuable data from danger.
Karen Kenworthy, Contributing Editor
WINDOWS MAGAZINE, **1999** , n 1006A, PG84
PUBLICATION DATE: 990615
JOURNAL CODE: WIN LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Build A Better Business
WORD COUNT: 3190

, **1999**
... a hash total) is also computed, based on this information. Finally, this hash total is **encrypted** using the **CA** 's **private key** . By **decrypting** the hash total, using the CA's public key and comparing it to the other...

17/3,K/18 (Item 2 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext

01095364 CMP ACCESSION NUMBER: CWK19960624S0146
Windows NT Server 4.0 Gets Enterprise Tools
Oliver Rist
COMMUNICATIONSWEEK, **1996** , n 616, PG76
PUBLICATION DATE: 960624
JOURNAL CODE: CWK LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Product Testing - First Look
WORD COUNT: 1128

, **1996**
... for Cryptography API), this feature will support all the most common encryption methods, including Data **Encryption** Standard and **public - key encryption** . It also supports **certification authority** , which means that it can handle digital signatures and transactions where one party is validated...

17/3,K/19 (Item 1 from file: 696)
DIALOG(R)File 696:DIALOG Telecom. Newsletters

00626994
OECD Tackles Digital Signatures Next Week In Ottawa
Electronic Mail & Messaging Systems
October 2,1998 VOL: 22 ISSUE: 18 DOCUMENT TYPE: NEWSLETTER
PUBLISHER: BRP PUBLICATIONS
LANGUAGE: ENGLISH WORD COUNT: 2413 RECORD TYPE: FULLTEXT

TEXT:
...Where governments have determined that digital signatures based on **public key cryptography** require **certification authorities** to support their functions on open networks, it is often asked whether certification authorities should...

1998

17/3,K/20 (Item 2 from file: 696)
DIALOG(R)File 696:DIALOG Telecom. Newsletters

00547665
CertCo, SPYRUS TO SUPPLY CRUCIAL SET CERTIFICATE AUTHORITY
Lisa Troshinsky, Associate Editor
Report on Smart Cards
May 26,1997 VOL: 11 ISSUE: 10 DOCUMENT TYPE: NEWSLETTER
PUBLISHER: BRP PUBLICATIONS
LANGUAGE: ENGLISH WORD COUNT: 905 RECORD TYPE: FULLTEXT

TEXT:
...s public key. For a third party to confirm someone's identity, it takes the **certifying authority** 's **public key** , **decrypts** the authenticating message and knows that someone (the certifying authority) has taken responsibility for assuring...

1997

17/3,K/21 (Item 3 from file: 696)
DIALOG(R)File 696:DIALOG Telecom. Newsletters

00059020
PACIFIC BELL EMBRACES THE INTERNET
Dan Amdur, Editor
Report on Electronic Commerce
April 30,1996 VOL: 3 ISSUE: 9 DOCUMENT TYPE: NEWSLETTER
PUBLISHER: BRP PUBLICATIONS
LANGUAGE: ENGLISH WORD COUNT: 1742 RECORD TYPE: FULLTEXT

TEXT:

...or Microsoft Exchange and the Business Transaction Network. The company also is looking at public/ **private encryption key** issues, and may act as **certifying authority** or as administrator for other companies' CA requirements...

1996

17/3,K/22 (Item 4 from file: 696)
DIALOG(R)File 696:DIALOG Telecom. Newsletters

00058905
LENDING A HELPING HAND TO THE WEB
Information & Interactive Services Report
May 3,1996 VOL: 17 ISSUE: 13 DOCUMENT TYPE: NEWSLETTER
PUBLISHER: BRP PUBLICATIONS
LANGUAGE: ENGLISH WORD COUNT: 799 RECORD TYPE: FULLTEXT

TEXT:
...or Microsoft Exchange and the Business Transaction Network. The company also is looking at public/ **private encryption key** issues, and may act as **certifying authority** or as administrator for other companies' certifying authority requirements...

1996

17/3,K/23 (Item 1 from file: 624)
DIALOG(R)File 624:McGraw-Hill Publications

0715516
Getting Smart with Intelligent Cards
Open Computing November 1995; Pg 15; Vol. 12, No. 11
Journal Code: UNIX ISSN: 0739-5922
Section Heading: OPENERS
Word Count: 618 *Full text available in Formats 5, 7 and 9*

BYLINE:
LEE BRUNO

Edited by Carolyn W.C. Wong with staff reports.

TEXT:
... focusing on home and small-business markets. ``Over the next 6 to 12 months, the **certification authorities** and **public key encryption** will be the biggest stumbling blocks."

1995

17/3,K/24 (Item 1 from file: 813)
DIALOG(R)File 813:PR Newswire

1405645 LAM073
New DST-Supported Initiative Resolves Interoperability Issues for Member Companies

DATE: January 18, 1999 17:31 EST WORD COUNT: 886

... dedicated to ensuring the privacy and authenticity of data communications enterprise-wide. Its award-winning **public - key** infrastructure technology combines **certification authority**, **encryption** and digital signature capabilities with fully automated key management. Used by financial institutions, government agencies...

17/3,K/25 (Item 2 from file: 813)
DIALOG(R)File 813:PR Newswire

1403961 DETH006
Leading Security Companies, Including Netrex, Outline Business Strategies And Emerging Technologies for Electronic Business

DATE: January 14, 1999 08:57 EST WORD COUNT: 849

... dedicated to ensuring the privacy and authenticity of data communications enterprise-wide. Its award-winning **public - key** infrastructure technology combines **certification authority** , **encryption** and digital signature capabilities with fully automated key management. Used by financial institutions, government agencies...

17/3,K/26 (Item 3 from file: 813)
DIALOG(R)File 813:PR Newswire

1210708 SFTU041
ARCANVS Becomes Licensed Certification Authority

DATE: January 13, 1998 13:52 EST WORD COUNT: 658

... avoid fraud and impersonation. ARCANVS is a Latin word which means something secretive and trustworthy. **Cryptography** involves **secret** , **private keys** . A **Certification Authority** which manages Certificates with integrity as a trusted third party is a publicly trustworthy service ...

17/3,K/27 (Item 1 from file: 553)
DIALOG(R)File 553:Wilson Bus. Abs. FullText

03072099 H.W. WILSON RECORD NUMBER: BWBA95072099 (USE FORMAT 7 FOR FULLTEXT)
The role of cryptography in network security.
Moore, Mitchell S
Business Communications Review (Bus Commun Rev) v. 25 (Sept. '95) p. 67-72
LANGUAGE: English
WORD COUNT: 3647

(USE FORMAT 7 FOR FULLTEXT)

TEXT:
... not only contains the user's public key, but also the authenticated identity of the **CA** .
Public key cryptosystems can also be used to provide an authentication service called "digital signature." Digital signatures permit...
1995

17/3,K/28 (Item 1 from file: 95)
DIALOG(R)File 95:TEME-Technology & Management

01301752 E99040843232
Hinter Schloss und Siegel. Sichere EMail durch S/MIME
Spiegel, G
c't, v38, n8, pp174-179, **1999**
Document type: journal article Language: German
Record type: Abstract
ISSN: 0724-8679

1999

ABSTRACT:
...und produktunabhaengig und plattformuebergreifend eine einheitliche Verfahrensweise zu manifestieren. S/MIME basiert auf auf CMS (**Cryptographic** Message Syntax), die im PKCS (**Public Key Cryptography** Standard) definiert ist. Eine **CA** (Certification Authority) bestaetigt mit ihrer digitalen Signatur die Authentizitaet von Benutzerschluesseln.
?

21/3,K/1 (Item 1 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

02360740 117541744
Digital signature management
Hassler, Vesna; Biely, Helmut
Internet Research v9n4 PP: 262-271 1999
ISSN: 1066-2243 JRNL CODE: NTRS
WORD COUNT: 5307

...TEXT: e-commerce. The project is currently in the implementation phase. In the first phase a **two** -level **CA** hierarchy will exist: a top-level CA and one end-user CA. This structure will...

... sufficient to ensure interoperability in this area. An IETF working group (PKIX, Internet X.509 **Public Key** Infrastructure) was established to specify the missing parts and in this way solve the interoperability...

21/3,K/2 (Item 2 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01782112 04-33103
Securing E-commerce sites
Buchner, Mark
Midrange Systems v12n3 PP: 28 Mar 1, 1999
ISSN: 1041-8237 JRNL CODE: MRS
WORD COUNT: 873

...TEXT: order to issue digital certificates to servers and users within their intranet. CAs broadcast their **public key** and Distinguished Name. People add them as trusted root key to Web servers and browsers. This means your server will trust anyone who has a certificate from that **CA** . There are **several** common CAs in the marketplace. Servers and browsers are shipped with several default trusted root...

21/3,K/3 (Item 3 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01698522 03-49512
PKI tames network security
McClure, Stuart
InfoWorld v20n37 PP: 65-66 Sep 14, 1998
ISSN: 0199-6649 JRNL CODE: IFW
WORD COUNT: 1568

...TEXT: Directory Access Protocol (LDAP) responds to requests to deliver the stored public key certificates.

The **CA** generates **two** separate pairs of public and **private keys** for each user or server. One pair is used for encrypting and decrypting information, and...

... this common problem: nonrepudiation. Nonrepudiation is the electronic equivalent of a signed log. Because the **CA** maintains **two** key pairs, the recipient of a digital signature, which was created with the sender's **private key** , can compare it to the signature generated by the receiver with the sender's **public key** . Thus, the recipient can confirm that the encrypted stream or file was actually made by...

21/3,K/4 (Item 4 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01397425 00-48412
Look who's joined the training game
Stamps, David
Training v34n3 PP: 32-38 Mar 1997
ISSN: 0095-5892 JRNL CODE: TBI
WORD COUNT: 2183

...TEXT: rental of all temp workers in the hands of a single vendor led to the **second** **key** el ement of the new employer-vendor relationship: on-premises contracts, in which account managers...

... of contracts in the industry today. "Staffing Industry Report," a newsletter based in Los Altos, **CA** , estimated as **many** as 3,000 onpremises contracts were in place at the end of 1996. For some...

21/3,K/5 (Item 1 from file: 810)
DIALOG(R)File 810:Business Wire

0754277 BW1271

ENTRUST TECHNOLOGIES: Entrust Technologies' Announces Solution for Secure Internet Banking and Brokerage

October 06, 1997

Byline: Business/Technology Editors

...of its Scotia OnLine service and has quickly become a leader in the issuance of **public - key** certificates from its **two** Entrust-based **Certification Authorities** .
Entrust/Direct is based on sound and proven cryptography, and allows customer to control their...

21/3,K/6 (Item 2 from file: 810)
DIALOG(R)File 810:Business Wire

0724271 BW1202

ENTRUST SCOTIABANK: Entrust Technologies and Scotiabank Enter Strategic Alliance to Develop Global Information Security Protection

July 16, 1997

Byline: Business Editors

...for this technology is "public-key cryptography." During the past two months, Scotiabank has implemented **two** " **Public - key Certification Authorities** ," enabling the bank to create and provide public-key certificates to users such as bank...

21/3,K/7 (Item 1 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext

01161939 CMP ACCESSION NUMBER: NWC19980515S0023
Fourth-Annual Well-Connected Awards: Enterprise Security
The Editors Of Network Computing
NETWORK COMPUTING, **1998** , n 909, PG106
PUBLICATION DATE: 980515
JOURNAL CODE: NWC LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Features
WORD COUNT: 1134

, 1998
... 888) VPNET-88, (408) 445-6600. www.vpnet.com

Key Management System

Xcert Software Sentry **CA**

There are **many** places to put your **public** **key** certificates, but Xcert Software's Sentry CA, our Well-Connected Award winner in Enterprise Security...

...Online Certificate Status Protocol), which may break down the barriers to a widely deployed, multivendor **public** **key** infrastructure.

Secure Parts Sentry CA has three components: an SSL (Secure Sockets Layer)-enabled Web...

21/3,K/8 (Item 1 from file: 696)
DIALOG(R)File 696:DIALOG Telecom. Newsletters

00702371
IDENTITY UNCERTAINTY STILL DOGS E-COMMERCE
ELECTRONIC COMMERCE NEWS
December 6, 1999 VOL: 4 ISSUE: 48 DOCUMENT TYPE: NEWSLETTER
PUBLISHER: PHILLIPS BUSINESS INFORMATION
LANGUAGE: ENGLISH WORD COUNT: 1550 RECORD TYPE: FULLTEXT

TEXT:
...that
their counterparts may be impostors, unauthorized agents or e-commerce Web sites being spoofed.
Public **key** infrastructure (PKI) technology goes a long way toward providing identity certainty. Through the power of...

...Kristin
Kupres, Identrus' chief operating and technology officer.
"Real-time validation capability within and across **public** **key** infrastructures is critical for businesses that intend to engage in high-value e-business transactions...processing loads, simplify end-user searches, and
eliminate the need to configure multiple clients to **multiple** **certification** **authorities** .
Under the OCSP protocol, relying parties send specific information about the certificates they receive to...

1999

21/3,K/9 (Item 2 from file: 696)
DIALOG(R)File 696:DIALOG Telecom. Newsletters

00625790
NACHA CA Interoperability Pilot Completes Phase I; Association Will Assess Findings Before Introducing Phase 2
Report on Smart Cards
September 28,1998 VOL: 12 ISSUE: 18 DOCUMENT TYPE: NEWSLETTER
PUBLISHER: BRP PUBLICATIONS
LANGUAGE: ENGLISH WORD COUNT: 448 RECORD TYPE: FULLTEXT

TEXT:
...As part of NACHA's Internet Council **CA** Interoperability Pilot, **several** security technology firms collaborated in making their digital

certificate systems interoperable to allows banks, merchants...

...Technologies. "The very nature of this pilot sends a clear message that CA and PKI [**public key** infrastructure] technology vendors are willing and able to collaborate in order to address interoperability issues associated with using **public - key** certificates...

1998

21/3,K/10 (Item 3 from file: 696)
DIALOG(R)File 696:DIALOG Telecom. Newsletters

00053522
SECURE GOVERNMENT TRANSACTION PILOT PLANNED TO BEGIN THIS MONTH
Report on Smart Cards
June 3,1996 VOL: 10 ISSUE: 11 DOCUMENT TYPE: NEWSLETTER
PUBLISHER: BRP PUBLICATIONS
LANGUAGE: ENGLISH WORD COUNT: 764 RECORD TYPE: FULLTEXT

TEXT:
...One major aspect of the project involves creating the **public key** infrastructure that will support this kind of verification, and the USPS has been developing a...that also want to act as certifying authorities - VeriSign Inc. and GTE Corp., to name **two** . As **certifying authority** , the USPS would issue digital IDs to users and verify that these digital stamps are...

1996

21/3,K/11 (Item 4 from file: 696)
DIALOG(R)File 696:DIALOG Telecom. Newsletters

00053329
SECURE GOVERNMENT TRANSACTION PILOT PLANNED TO BEGIN IN JUNE
Report on Electronic Commerce
May 28,1996 VOL: 3 ISSUE: 11 DOCUMENT TYPE: NEWSLETTER
PUBLISHER: BRP PUBLICATIONS
LANGUAGE: ENGLISH WORD COUNT: 777 RECORD TYPE: FULLTEXT

TEXT:
One major aspect of the project involves creating the **public key** infrastructure that will support this kind of verification, and the USPS has been developing a...

...that also want to act as certifying authorities - VeriSign Inc. and GTE Corp., to name **two** . As **certifying authority** , the USPS would issue digital IDs to users and verify that these digital stamps are...

1996

21/3,K/12 (Item 1 from file: 813)
DIALOG(R)File 813:PR Newswire

1406326 LATU028
Digital Signature Trust Company Validates Concept of Industry-Wide Certificate Authority in Securities Industry Pilot

DATE: January 19, 1999 13:00 EST WORD COUNT: 884

...root CA for the pilot. As a part of ABAecom's offer, DST provided the **public key** infrastructure (PKI) behind the root CA for SIRCA. DST also collaborated with the National Association...

... signing process with the respective PKI technologies used by the firms. Additionally, DST provided the **CA** operation for **two** of the participating firms.

"As our world becomes increasingly electronic, the necessity to facilitate secure...

21/3,K/13 (Item 1 from file: 553)
DIALOG(R)File 553:Wilson Bus. Abs. FullText

04047836 H.W. WILSON RECORD NUMBER: BWBA99047836 (USE FORMAT 7 FOR FULLTEXT)
Knock, knock . . . who's there?.
AUGMENTED TITLE: public key encryption
Rothman, Mike
Communications News v. 36 no6 (June 1999) p. 28-9
LANGUAGE: English
WORD COUNT: 1522

(USE FORMAT 7 FOR FULLTEXT)

TEXT:
... IN A SECURE BUSINESS TRANSACTION
1 A trusted third party known as a certificate authority (**CA**) issues **two** keys: a **private key** to an individual and a **public key** validated by the CA accessible to the general public. The CA can be internal to...
1999
?

```
Set      Items   Description
S1          64   AU= (CORDERY R? OR CORDERY, R?)
S2          14   CERTICOM
S3        4617   ELLIPTIC(2N)CURV? OR HYPERELLIPTIC(2N)CURV?
S4        2534   (PRIVAT? OR PUBLIC?OR SECRET? OR FIRST OR SECOND? OR PRIMA-
                 R?)(1W) KEY? ?
S5     1177994   HCC OR AVC OR CODIF? OR DECOD? OR UNENCOD? OR DECRYPT? OR -
                 UNENCRYPT? OR UNCRYPT? OR CIPHER? OR CYPHER? OR ENCOD? OR COD-
                 E? ? OR CODING? OR ENCOD? OR ENCIPHER? OR ENCYPHER? OR UNCOD?
                 OR DECIPHER? OR DECYPHER? OR UNENCIPHER? OR UNENCYPHER?
S6      114235   UNCIPHER? OR UNCYPHER? OR CRYPTO? OR ENCRYPT?
S7     1122170   CERTIFYING? OR CERTIFY OR CERTIFICATION? OR CERTIFIES OR C-
                 ONFIRM? OR VERIFY? OR ATTEST?
S8     6556343   STATION? OR AUTHORIT? OR POWER? OR AGENC? OR ORGANI? OR BO-
                 ARD?
S9    16006517   MULTI? OR PLURAL? OR MANY OR SEVERAL? OR NUMER? OR CLUSTER?
                  OR GROUP? OR MULTIPL? OR PLENTY? OR CONSIDERABLE? OR TWO OR -
                 DUAL OR DOUBL?
S10          4   S2 AND S3
S11          4   RD (unique items)
S12         23   S4 AND (S5 OR S6) AND (S7(3N)S8)
S13         19   RD (unique items)
S14         12   S13 AND PY<=1999
S15         32   S4 AND S9 AND S7 AND S8
S16         26   RD (unique items)
S17         19   S16 NOT S12
S18         12   S17 AND PY<=1999
S19          0   S1 AND S4 AND (S5 OR S6)
S20         12   S4 AND (S5 OR S6) AND S7 AND S8 AND S9
S21          5   S20 NOT (S18 OR S14 OR S10)
S22          5   RD (unique items)
S23          0   S22 AND PY<=1999
? show files
File 238:Abs. in New Tech & Eng. 1981-2002/Jul
         (c) 2002 Cambridge Scient. Abstr
File   8:Ei Compendex(R) 1970-2002/Aug W2
         (c) 2002 Engineering Info. Inc.
File  77:Conference Papers Index 1973-2002/Jul
         (c) 2002 Cambridge Sci Abs
File  35:Dissertation Abs Online 1861-2002/Jul
         (c) 2002 ProQuest Info&Learning
File 202:Information Science Abs. 1966-2002/Jul 03
         (c) Information Today, Inc
File   2:INSPEC 1969-2002/Aug W2
         (c) 2002 Institution of Electrical Engineers
File 233:Internet & Personal Comp. Abs. 1981-2002/Aug
         (c) 2002 Info. Today Inc.
File  94:JICST-EPlus 1985-2002/Jun W3
         (c)2002 Japan Science and Tech Corp(JST)
File   6:NTIS 1964-2002/Aug W4
         (c) 2002 NTIS, Intl Cpyrght All Rights Res
File 144:Pascal 1973-2002/Aug W2
         (c) 2002 INIST/CNRS
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File  62:SPIN(R) 1975-2002/Jul W2
         (c) 2002 American Institute of Physics
File  99:Wilson Appl. Sci & Tech Abs 1983-2002/Jun
         (c) 2002 The HW Wilson Co.
File  34:SciSearch(R) Cited Ref Sci 1990-2002/Aug W2
         (c) 2002 Inst for Sci Info
?
```

11/3,K/1 (Item 1 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00660370 02CW04-011
FAA adopts wireless encryption for safety
Verton, Dan
Computerworld , April 1, 2002 , v36 n14 p10, 1 Page(s)
ISSN: 0010-4841
Company Name: **Certicom**

Company Name: **Certicom**
... licensing wireless encryption technology. Explains that FAA will license public key infrastructure (PKI) technology from **Certicom** Corp. of Hayward, CA. Mentions that the move comes as the FAA enters the implementation...

... into the data link between ground controllers and pilots. Notes the ATN will rely on **Certicom** 's **Elliptic Curve** Cryptography, a standard for digital signature algorithms that offers more efficient use of bandwidth than...
Identifiers: **Certicom**

11/3,K/2 (Item 2 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00614782 00CW11-301
MicroStrategy, Aether to take data mining wireless
Weiss, Todd R
Computerworld , November 27, 2000 , v34 n48 p66, 1 Page(s)
ISSN: 0010-4841
Company Name: MicroStrategy; Aether Systems

...any wireless network. Indicates that wireless security is provided by a mechanism based on the **Elliptic Curve** Cryptosystem developed by **Certicom** Corp. of Hayward, CA. Explains that AIM supports most operating systems and portable devices. Includes...

11/3,K/3 (Item 3 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00602973 00IK05-015
Pocket PC secured for e-biz
Yasin, Rutrell
InternetWeek , May 1, 2000 , n811 p31, 1 Page(s)
ISSN: 0746-8121
Company Name: TD Waterhouse; Microsoft
Product Name: Microsoft Pocket PC

... with traders. Enumerates the features of the rival Palm platform, such as use of the **Elliptic Curve** Cryptography technol from **Certicom** Corp., Message Integrity Check which detects transmission errors, and network authentication. Includes a photo. (MEM)

11/3,K/4 (Item 1 from file: 99)
DIALOG(R)File 99:Wilson Appl. Sci & Tech Abs

2442660 H.W. WILSON RECORD NUMBER: BAST98016290
Encryption battle heats up
Computer v. 31 (Jan. 1998) p. 22
DOCUMENT TYPE: Feature Article ISSN: 0018-9162

...ABSTRACT: of a strong, fast 128-bit encryption technology. Moreover,

several companies have begun to deploy **Certicom** 's **elliptic - curve** cryptography, which uses fewer computations than S/MIME.
?

14/3,K/1 (Item 1 from file: 238)
DIALOG(R)File 238:Abs. in New Tech & Eng.

0319909 ANTE NUMBER: 83769
Signing away the future
AUTHOR(S): Harrington, T.
JOURNAL: Computing 11 Mar 1999 p.53-4, 56.
PUBLICATION YEAR: **1999**
ISSN: 0144-3097
BLDSC SHELF MARK: 3395.009
LANGUAGE: English

PUBLICATION YEAR: **1999**

ABSTRACT: ...with regard to digital signatures for online transactions is examined. Problems in the UK with **encryption** , public/ **private key cryptography** , and **certifying authorities** (trusted third parties) are discussed, and compared to the situation in other European countries and...

14/3,K/2 (Item 1 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

04665354 E.I. No: EIP97043595398
Title: Inferno security
Author: Presotto, David Leo
Corporate Source: Bell Labs
Conference Title: Proceedings of the 1997 IEEE COMPCON Conference
Conference Location: San Jose, CA, USA Conference Date: 19970223-19970226
E.I. Conference No.: 46226
Source: Digest of Papers - COMPCON - IEEE Computer Society International Conference 1997. IEEE, Piscataway, NJ, USA,97CB36028. p 251-253
Publication Year: 1997
CODEN: DCSIDU
Language: English

...Abstract: optional: an application may use it or avoid it. Inferno provides strong mutual authentication, message **encryption** , message digesting, and digital signatures. Authentication and digital signatures are performed using public key **cryptography** . Public keys are certified by Inferno-based **certifying authorities** that sign the public keys with their own **private key** . (Author abstract) 7 Refs.
Descriptors: Security of data; Computer operating systems; **Cryptography** ; Algorithms; Data communication systems; Network protocols; Data processing

14/3,K/3 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC

6498703 INSPEC Abstract Number: B2000-03-6120D-084, C2000-03-6130S-044
Title: On the life cycle of the certification authority **key pair in EMV 96**
Author(s): Markantonakis, C.; Rantos, K.
Author Affiliation: Inf. Security Group, London Univ., Egham, UK
Conference Title: EUROMEDIA '99 p.125-30
Editor(s): Hahn, W.; Walther-Klaus, E.; Knop, J.
Publisher: SCS, San Diego, CA, USA
Publication Date: 1999 Country of Publication: USA x+256 pp.
ISBN: 1 56555 169 9 Material Identity Number: XX-2000-00187
Conference Title: EUROMEDIA'99
Conference Sponsor: Siemens AG
Conference Date: 26-28 April 1999 Conference Location: Munich, Germany
Language: English

Subfile: B C
Copyright 2000, IEE

Title: On the life cycle of the certification authority **key pair in EMV 96**
...Abstract: namely that there are no provisions for dealing with the compromise or revocation of the **certification authority** 's **private key** . We believe that in such a case the whole system would collapse. An attacker possessing...

... by re-issuing the old cards and setting up the ICC terminals with the new **certification authority** (CA) public key. Our proposed solution aims to extend the system's life cycle, i...
...Descriptors: public key **cryptography**
...Identifiers: **certification authority** ; ...

... **private key** ;
1999

14/3,K/4 (Item 2 from file: 2)
DIALOG(R)File 2:INSPEC

6496455 INSPEC Abstract Number: B2000-03-6120D-071, C2000-03-1260C-049
Title: A global key recovery system
Author(s): Lein Harn; Hung-Yu Lin; Guang Gong
Author Affiliation: Dept. of Comput. Networking, Missouri Univ., Kansas City, MO, USA
Conference Title: Proceedings of 1999 International Workshop on Cryptographic Techniques and E-Commerce p.81-5
Editor(s): Blum, M.; Lee, C.H.
Publisher: City Univ. Hong Kong, Kowloon, Hong Kong
Publication Date: 1999 Country of Publication: Hong Kong x+290 pp.
ISBN: 962 937 049 2 Material Identity Number: XX-1999-02077
Conference Title: Proceedings of CrypTEC'99: International Workshop on Cryptographic Techniques and E-Commerce
Conference Date: 5-8 July 1999 Conference Location: Hong Kong
Language: English
Subfile: B C
Copyright 2000, IEE

Abstract: **Cryptographic** technologies used today are either symmetric key or public key. **Cryptographic** keys have become vital parts in modern communications. Key recovery is a technology that allows the owner of **encrypted** data or a trusted third party to recover a lost or otherwise unavailable session key. Key recovery has emerged as a safe, practical method for recovering **encrypted** data. We propose a key recovery system that combines the functions of public-key **certification** and key recovery **authorities** . This key recovery system recovers a user's **private key** that is used to generate digital signatures or to **encrypt** random session keys. This proposed system is easy to implement, scalable, has no single point...
...Descriptors: public key **cryptography**
...Identifiers: symmetric key **cryptography** ; ...

...public key **cryptography** ; ...

... **encrypted** data
1999

14/3,K/5 (Item 3 from file: 2)
DIALOG(R)File 2:INSPEC

6137991 INSPEC Abstract Number: B1999-02-6120D-050, C1999-02-6130S-070
Title: Key management unit CK-Guard
Author(s): Hosokawa, T.; Miyauchi, H.; Kimura, M.

Author Affiliation: Data Commun. Div., NEC Corp., Japan
Journal: NEC Technical Journal vol.51, no.9 p.146-9
Publisher: NEC,
Publication Date: Sept. 1998 Country of Publication: Japan
CODEN: NECGEZ ISSN: 0285-4139
SICI: 0285-4139(199809)51:9L.146:MUG;1-P
Material Identity Number: H719-1998-012
Language: Japanese
Subfile: B C

Abstract: Management of **private keys** is a crucial issue in systems which require high-level security, such as **certification authorities** based on the RSA public key **cryptosystem** . NEC has developed tamper resistant **private key** management equipment, CK-Guard. CK-Guard is accessed by software Secureware/ **Private Key** Module Manager on the server connected with the CK-Guard. The users can manage CK...
...Descriptors: **cryptography** ;
...Identifiers: **private key** management...

... **certification authorities** ; ...

...RSA public key **cryptosystem** ; ...

...tamper resistant **private key** management...

... **Private Key** Module Manager
1998

14/3,K/6 (Item 4 from file: 2)
DIALOG(R)File 2:INSPEC

5533606 INSPEC Abstract Number: C9705-6130S-013
Title: Legal signatures and proof in electronic commerce
Author(s): Wright, B.
Conference Title: Proceedings of the Second USENIX Workshop on Electronic Commerce p.67-75
Publisher: USENIX Assoc, Berkeley, CA, USA
Publication Date: 1996 Country of Publication: USA vi+314 pp.
Material Identity Number: XX96-03462
Conference Title: Proceedings of 2nd USENIX Workshop on Electronic Commerce
Conference Sponsor: USENIX Assoc.; Univ. California Berkley
Conference Date: 18-21 Nov. 1996 Conference Location: Oakland, CA, USA
Language: English
Subfile: C

...Abstract: of Utah (USA) has enacted a scheme for certifying a public key through a licensed **certification authority** . The Utah scheme concentrates risk in the **private key** . In contrast, the IRS (Internal Revenue Service) is using a biometric signature technology called PenOp...
...Descriptors: public key **cryptography** ;
...Identifiers: licensed **certification authority** ; ...

... **private key** ;
1996

14/3,K/7 (Item 5 from file: 2)
DIALOG(R)File 2:INSPEC

4906923 INSPEC Abstract Number: B9505-6120B-003, C9505-6130S-003
Title: Issues in using public-key cryptography **in signing electronic documents**
Author(s): Wright, B.

Journal: EDPACS vol.22, no.9 p.9-12
Publication Date: March 1995 Country of Publication: USA
CODEN: EDPCDF ISSN: 0736-6981
Language: English
Subfile: B C

Title: Issues in using public-key cryptography **in signing electronic documents**

Abstract: Public-key **cryptography** was developed by A. Shamir (1978) as a means for authenticating electronic messages. Public-key **cryptography** is intended to be employed in marking computer data so that the integrity and origin...

...proven. This article examines some of the issues associated with the use of public-key **cryptography** in signing or authenticating electronic documents. Using a public-key **cryptography** scheme seems to be an impressive way to achieve airtight legal proof of who agreed...

... in electronic commerce. However, the implementation of this seemingly airtight scheme has four problems: (i) **private keys** are hard to manage; (ii) smart card technology costs something; (iii) standards are necessary; and (iv) public keys are hard to manage. When public-key **cryptography** employing a **certification authority** is used to sign a legal document, the parties to the transaction are seeking to...

... a secure record. Depending on how they are implemented, the various forms of public key **cryptography** can perform some or all of the functions described in this article. This discussion of public-key **cryptography** does not refer to any particular commercial product or implementation of it.

...Descriptors: public key **cryptography** ;
Identifiers: public-key **cryptography** ; ...

... **private keys** ; ...

... **certification authority** ;
1995

14/3,K/8 (Item 1 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00525091 99WI02-003
E-commerce: digital signature technology
Zhou, Tao
Windows NT , February 1, 1999 , n42 p75-80, 5 Page(s)
ISSN: 1083-138X

Describes digital signature technology and its role in electronic commerce. Explains message hashing and **encryption** , how public and **private keys** work, and two public key trust models, direct and third-party. Discusses how the third-party model uses the Certificate Authority (CA), a trustworthy **organization** that **certifies** public keys and publishes the Certificate Revocation List (CRL). Examines the use of time stamping...
1999

14/3,K/9 (Item 1 from file: 94)
DIALOG(R)File 94:JICST-EPlus

03634839 JICST ACCESSION NUMBER: 98A0601240 FILE SEGMENT: JICST-E
Verification of public key certificates.
SAKAKIBARA HIROYUKI (1); YOSHITAKE JUN (1)
(1) Mitsubishi Electric Corp.
Joho Shori Gakkai Kenkyu Hokoku, **1998** , VOL.98,NO.54(CSEC-1), PAGE.53-58,

FIG.5, REF.4
JOURNAL NUMBER: Z0031BAO ISSN NO: 0919-6072
UNIVERSAL DECIMAL CLASSIFICATION: 681.3.02.001 681.3.02-759
LANGUAGE: Japanese COUNTRY OF PUBLICATION: Japan
DOCUMENT TYPE: Journal
ARTICLE TYPE: Original paper
MEDIA TYPE: Printed Publication

, **1998**
ABSTRACT: Recently requirement of public key **cryptosystem** has been increased on the Internet communication. A "public key certificate" issued by a **Certification Authority** (CA) is needed for secure communication with public key **cryptosysytem** . A public key certificate is data structure which binds public key value to the public key owner digitally signed with the CA's **private key** . A public key of an entity should be safely obtained from the certificate verified through ...
...DESCRIPTORS: public key **cryptography** ;
...BROADER DESCRIPTORS: **cryptogram** ;

14/3,K/10 (Item 1 from file: 6)
DIALOG(R)File 6:NTIS

1935288 NTIS Accession Number: DE96000777
Public/ private key certification authority **and key distribution. Draft**
Long, J. P. ; Christensen, M. J. ; Sturtevant, A. P. ; Johnston, W. E.
Sandia National Labs., Albuquerque, NM.
Corp. Source Codes: 068123000; 9511100
Sponsor: Department of Energy, Washington, DC.
Report No.: SAND-95-2147C-DRAFT; CONF-9509224-1-DRAFT
25 Sep 95 25p
Languages: English Document Type: Conference proceeding
Journal Announcement: GRAI9608; ERA9610
Joint meeting of Energy Science Coordinating Committee, Newport News, VA (United States), 28-29 Sep 1995. Sponsored by Department of Energy, Washington, DC.
Order this product from NTIS by: phone at 1-800-553-NTIS (U.S. customers); (703)605-6000 (other countries); fax at (703)321-8547; and email at orders@ntis.fedworld.gov. NTIS is located at 5285 Port Royal Road, Springfield, VA, 22161, USA.
NTIS Prices: PC A03/MF A01

Public/ private key certification authority **and key distribution. Draft**
Traditional **encryption** , which protects messages from prying eyes, has been used for many decades. The present concepts of **encryption** are built from that heritage. Utilization of modern software-based **encryption** techniques implies much more than simply converting files to an unreadable form. Ubiquitous use of computers and advances in **encryption** technology coupled with the use of wide-area networking completely changed the reasons for utilizing **encryption** technology. The technology demands a new and extensive infrastructure to support these functions. Full understanding...

... paper addresses issues surrounding the establishment and operation of a key management system (i.e., **certification authority**) that is essential to the successful implementation and wide-spread use of **encryption** .
Descriptors: Computer Networks; **Cryptography** ; Data Transmission; Security; Meetings

14/3,K/11 (Item 1 from file: 144)
DIALOG(R)File 144:Pascal

14056149 PASCAL No.: 99-0246867
A prototype implementation of a system to support multiple certification

authorities
Global IT security : Vienna, Budapest, 31 August - 2 September 1998
CHANG H
PAPP Gyoergy, ed; POSCH Reinhard, ed
PIPSC, 530 Laurier Avenue West, Ottawa, K1R 7T1, Canada
IFIP TC11 conferenceSEC '98 : international conference on information security, 14IFIP TC11 conferenceSEC '98 : international conference on information security, 14 (Budapest HUN) 1998-08-31
1998 504-508
Publisher: OCG, Vienna; IFIP, Vienna
Language: English

A prototype implementation of a system to support multiple certification authorities
1998
... 509 specifies a property that both keys in the key pair can be used for **encipherment** , with the **private key** being used to **decipher** if the public key was used, and the public key being used to **decipher** if the **private key** was used. An extension to X.509 could be used for implementation of a multiple **Certification Authorities** (CAs) system. Our system can be used for implementation of multiple certificate policies. It can be used also for distribution of public keys for **encryption** as well as for public keys for verification of digital signature. To improve interoperability, certificates...

English Descriptors: **Cryptography** ; Public key; Certification; Authentication; Signing; Service quality; Prototype; Implementation; Electronic data interchange

French Descriptors: **Cryptographie** ; Cle publique; Certification; Authentification; Signature; Qualite service; Prototype; Implementation; Echange donnee informatise

14/3,K/12 (Item 1 from file: 99)
DIALOG(R)File 99:Wilson Appl. Sci & Tech Abs

1675632 H.W. WILSON RECORD NUMBER: BAST96064609
Digital signatures
AUGMENTED TITLE: VeriSign
Garfinkel, Simson L;
Technology Review v. 99 (Nov./Dec. '96) p. 14-15
DOCUMENT TYPE: Feature Article ISSN: 0040-1692

ABSTRACT: New organizations called certificate authorities are using digital signatures to **encrypt** messages on the Internet so that they cannot be read by anyone other than the...

...and not to a digital impostor, but, for an annual fee, VeriSign, the largest certificate **authority** , will **confirm** that a public key really belongs to a particular individual or company. Concern that **encryption** may be used to evade court-authorized wiretaps has prompted the U.S. government to adopt the Digital Signature Standard (DDS). DDS allows the use of public and **private keys** for digital signature but not for **encryption** .
1996
?

18/3,K/1 (Item 1 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

04509992 E.I. No: EIP96093348271
Title: Integration of magnetic bearings in the design of advanced gas turbine engines
Author: Storace, A.F.; Sood, D.; Lyons, J.P.; Preston, M.A.
Corporate Source: General Electric Co, Cincinnati, OH, USA
Source: Journal of Engineering for Gas Turbines and Power, Transactions of the ASME v 117 n 4 Oct 1995. p 655-665
Publication Year: 1995
CODEN: JETPEZ ISSN: 0742-4795
Language: English

...Abstract: gas turbine engine rotor support. These advantages include tremendously improved vibration and stability characteristics, reduced **power** loss, improved reliability, fault tolerance, and greatly extended bearing service life. The marriage of these...

...performance and structural efficiency for future gas turbine engines. However, obtaining the maximum payoff requires **two** key ingredients. The first is the use of modern magnetic bearing technologies such as innovative digital control techniques, high-density **power** electronics, high-density magnetic actuators, fault-tolerant system architecture, and electronic (sensorless) position estimation. This paper describes these technologies and the test hardware currently in place for **verifying** the performance of advanced magnetic actuators, **power** electronics, and digital controls. The **second key** ingredient is to go beyond the simple replacement of rolling element bearings with magnetic bearings...
Descriptors: Gas turbines; Magnetic bearings; Technology; Digital control systems; **Power** electronics; Actuators; Fault tolerant computer systems; Composite materials; Aircraft materials

18/3,K/2 (Item 1 from file: 35)
DIALOG(R)File 35:Dissertation Abs Online

01426864 ORDER NO: AADAA-INN95626
THE DESIGN OF SUBSTITUTION-PERMUTATION NETWORK CIPHERS RESISTANT TO CRYPTANALYSIS
Author: HEYS, HOWARD M.
Degree: PH.D.
Year: **1994**
Corporate Source/Institution: QUEEN'S UNIVERSITY AT KINGSTON (CANADA) (0283)
Source: VOLUME 56/04-B OF DISSERTATION ABSTRACTS INTERNATIONAL. PAGE 2212. 163 PAGES
ISBN: 0-315-95626-7

Year: **1994**

In this thesis, we examine a fundamental class of **private key** block ciphers, referred to as substitution-permutation networks (SPNs). In particular, we study design principles...

...that is applicable to all classes of SPNs. As well, we consider the application of two established, **powerful** attacks: differential cryptanalysis and linear cryptanalysis. We find that the appropriate selection of S-boxes...

...the avalanche criterion and relate the key avalanche property to the application of a key **clustering** attack. The results of the analysis further **confirm** the general design principles suggested above.

18/3,K/3 (Item 2 from file: 35)
DIALOG(R)File 35:Dissertation Abs Online

01370716 ORDER NO: AAD94-22762
CONNECTIVITY IN RANDOM NETWORKS AND TRAFFIC MODELING IN MOBILE NETWORKS
Author: WENG, LIN
Degree: D.SC.
Year: **1994**
Corporate Source/Institution: THE GEORGE WASHINGTON UNIVERSITY (0075)
Source: VOLUME 55/04-B OF DISSERTATION ABSTRACTS INTERNATIONAL.
PAGE 1595. 168 PAGES

Year: **1994**

...thesis we consider a novel approach to connectivity analysis in a packet radio network. A **second** **key** contribution is a **powerful** analytic tool for traffic modeling in mobile networks.

The connectivity analysis includes an extension of Erdos single link random Euclidean networks to a general **multiple** hop network. The importance of this approach is its generalization to a future network concept which may have mobile base **stations** or the mobiles themselves become relay **stations** in the network. We characterize the minimum path length distribution (MPLD) between nodes, defined as...
...we investigate some applications of MPLD. The MPLD is a fundamental problem that applies to **many** aspects of network analysis, such as the connectivity, **power** assignment, routing criteria, average time delay, etc.

The traffic modeling of mobile networks combines **several** important features including non-uniform cross boundary traffic, and specific road map characteristics which influence the mobile dynamics. From this model and assumed distributions we derive **several** performance criteria including handoff probability, stay-in cell time distribution, blocking probability and a new...

...can be examined analytically, again eliminating entire simulation runs.

The simulations have been presented to **verify** the validity of the assumptions and approximations made in the analysis.

18/3,K/4 (Item 3 from file: 35)
DIALOG(R)File 35:Dissertation Abs Online

01233039 ORDER NO: AAD92-15566
STUDIES OF THE TOTAL SYNTHESIS OF FREDERICAMYCIN A. DEVELOPMENT OF AN INTERMOLECULAR ALKYNE-CHROMIUM CARBENE BENZANNULATION APPROACH TO THE ABCD(E) RING SYSTEM: PREPARATION OF ABCD, ABCDE AND FULLY FUNCTIONALIZED ABCDE STRUCTURAL ANALOGS (CHROMIUM CARBENE BENZANNULATION)
Author: JACOBSON, IRINA CIPORA
Degree: PH.D.
Year: **1991**
Corporate Source/Institution: PURDUE UNIVERSITY (0183)
Source: VOLUME 53/03-B OF DISSERTATION ABSTRACTS INTERNATIONAL.
PAGE 1370. 201 PAGES

Year: **1991**
Descriptors: CHEMISTRY, **ORGANIC**

...highly unusual structure, isolated from Streptomyces griseus, exhibits very good in vitro cytotoxic activity and **confirmed** antibacterial and antifungal activity. In vivo, it exhibits significant antitumor activity. The syntheses of ABCD...

...highly convergent approach to the synthesis of Fredericamycin A is based on implementation of the **two** key carbon-carbon bond forming steps with the rest being functional **group** interconversions and/or protection/deprotection. The **first** **key** carbon-carbon bond forming step is the regiospecific alkyne-chromium carbene benzannulation reaction that introduces...

18/3,K/5 (Item 4 from file: 35)
DIALOG(R)File 35:Dissertation Abs Online

1070192 ORDER NO: AAD89-18989
PRODUCTIVITY MEASUREMENT AND ENHANCEMENT IN NAVAL AIRCRAFT INTERMEDIATE MAINTENANCE DEPARTMENTS: A STUDY OF THE METHODOLOGY FOR GENERATING EFFICIENCY AND EFFECTIVENESS MEASURES
Author: ORTON, FREDERICK CHARLES
Degree: D.B.A.
Year: **1989**
Corporate Source/Institution: UNITED STATES INTERNATIONAL UNIVERSITY (0239)
Source: VOLUME 50/05-A OF DISSERTATION ABSTRACTS INTERNATIONAL. PAGE 1369. 189 PAGES

Year: **1989**

...investigate the inter-service transportability of this technology. Method. The research design consisted of selecting **two** major shore-based Naval Aircraft Intermediate Departments (AIMDs) under the Commander, Naval Air Force, United...

...MGEEM: the other AIMD served as the control facility for the experiment. To answer the **second** question, **Key** Result Areas (KRAs), indicators and the related changes in productivity were compared with an independently-conducted implementation in an Air Force facility with an identical **organizational** mission.
Results. The findings of this study **confirmed** the viability of using the MGEEM in Naval industrial facilities, since productivity increased 43.7 ...

...measurement and enhancement model would be required to better fit the system to the specific **organization** .

18/3,K/6 (Item 5 from file: 35)
DIALOG(R)File 35:Dissertation Abs Online

0975833 ORDER NO: AAD87-29049
SYNTHESIS OF A DEGRADATION PRODUCT OF ANADENSIN
Author: WISSINGER-CORNILLE, JANE E.
Degree: PH.D
Year: **1987**
Corporate Source/Institution: NORTHWESTERN UNIVERSITY (0163)
Source: VOLUME 48/10-B OF DISSERTATION ABSTRACTS INTERNATIONAL. PAGE 2981. 165 PAGES

Year: **1987**
Descriptors: CHEMISTRY, **ORGANIC**

...the anionic oxy-Cope rearrangement of dialkenylcyclobutanols for stereospecific formation of the cyclooctane ring. The **first** **key** intermediate targeted for synthesis was (1$\beta,4\beta,5\beta)$-5-ethenyl-1-methyl...

...state afforded the 1α-isopropyl-3a$\beta{,}7\beta$-dimethylcyclopentacyclooctenone. Isomerization of the cyclooctenone **double** bond followed by hydrogenation produced the required trans-fused-β-isopropylcyclooctanone. Cyclopentenone annulation of this...

...dicyclopenta (a,d) cycloocten-2-one synthesized with identical to the product produced from a **two** step degradation of an authentic sample of anadensin. An X-ray crystal structure of the 5-8-5 cyclopentenone identified the 3a stereochemistry and **confirmed** its molecular structure as an advanced intermediate towards the synthesis of anadensin.

18/3,K/7 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC

6444461 INSPEC Abstract Number: B2000-02-6120D-011
Title: A new two -way and location-secure authentication scheme based on secret sharing
Author(s): Shiuh-Jeng Wang; Ywh-Ren Tsai; Jin-Fu Chang
Author Affiliation: Dept. of Inf. Manage., Central Police Univ., Taoyuan, Taiwan
Journal: Journal of the Chinese Institute of Electrical Engineering vol.6, no.4 p.293-305
Publisher: Chinese Inst. Electr. Eng., Taiwan,
Publication Date: Nov. 1999 Country of Publication: Taiwan
CODEN: ZDIGEK ISSN: 1023-4462
SICI: 1023-4462(199911)6:4L.293:LSAS;1-C
Material Identity Number: F162-1999-003
Language: English
Subfile: B

Title: A new two -way and location-secure authentication scheme based on secret sharing
...Abstract: The proposed scheme is based on the technique of secret sharing via the use of **private keys** . Handoff is a phenomenon very unique in mobile communications. Authentication is not only needed during ...

... authentication to be done in both occasions. The scheme has the additional attractions of providing **two** -way authentication and location privacy. **Two** -way authentication allows a base **station** and a mobile unit to **verify** each other. Location privacy is a feature becoming increasingly attractive to **many** subscribers.
...Identifiers: **two** -way authentication scheme...

... **private keys** ;
1999

18/3,K/8 (Item 2 from file: 2)
DIALOG(R)File 2:INSPEC

4917167 INSPEC Abstract Number: C9505-3390C-029
Title: The development of a fully autonomous ground vehicle (FAGV)
Author(s): Gomi, T.; Ide, K.-I.; Matsuo, H.
Author Affiliation: Appl. AI Syst. Inc., Kanata, Ont., Canada
p.62-7
Publisher: IEEE, New York, NY, USA
Publication Date: 1994 Country of Publication: USA xii+611 pp.
ISBN: 0 7803 2135 9
Conference Title: Proceedings of the Intelligent Vehicles '94 Symposium
Conference Sponsor: IEEE Ind. Electron. Soc
Conference Date: 24-26 Oct. 1994 Conference Location: Paris, France
Language: English
Subfile: C

...Abstract: environment without any external guidance. The crucial technique employed is a non-Cartesian way of **organizing** software agents for the creation of a highly responsive control program. The resulting software is considerably reduced in size. Through **numerous** experiments using mobile robots we **confirmed** that these new control programs excel in functionality, efficiency, flexibility and robustness. The **second key** technique in the planning stage is evolutionary computation, of which genetic algorithms are a principal...
1994

18/3,K/9 (Item 1 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00510416 98IX10-002
All eyes on PKI -- Though still in its infancy, PKI is already being heralded for its strength and versatility. But can it withstand the weight of our...
Bhimani, Anish
Information Security , October 1, 1998 , v1 n11 p22-31, 5 Page(s)
ISSN: 1096-8903

... key infrastructure (PKI), which allows users to interact with other users and applications, obtain and **verify** identities and keys, and register with certificate **authorities** . Describes the components needed to take full advantage of PKI, including certificate **authority** (CA), root CA, registration **authority** , certificate directory, management protocols, operational protocols, and personal security environment. Attention is given to such deployment issues as verification procedures, the scope of **certification** , certificate lifetimes, and the validation of certificates. Considers outsourcing with regard to deploying PKIs to...

... to widespread PKI usage is the lack of interoperability and standards. Also discusses protecting the **private key** in electronic transactions. Includes **two** sidebars and three diagrams. (jo)
1998
Descriptors: Electronic Commerce; Security; Internet; Certificate **Authorities**

18/3,K/10 (Item 1 from file: 6)
DIALOG(R)File 6:NTIS

2116884 NTIS Accession Number: PB99-122129/XAB
Residential Wood Combustion Technology Review. Volume 2. Appendices
(Final rept. Jul 97-Jul 98)
Houck, J. E. ; Tiegs, P. E.
OMNI Environmental Services, Inc., Beaverton, OR.
Corp. Source Codes: 089645000
Sponsor: Environmental Protection Agency, Research Triangle Park, NC. Air Pollution Prevention and Control Div.
Report No.: EPA/600/R-98/174B
Dec 1998 186p
Languages: English
Journal Announcement: GRAI9911
See also Volume 1, PB99-122111. Sponsored by Environmental Protection Agency, Research Triangle Park, NC. Air Pollution Prevention and Control Div.
Product reproduced from digital image. Order this product from NTIS by: phone at 1-800-553-NTIS (U.S. customers); (703)605-6000 (other countries); fax at (703)605-6900; and email at orders@ntis.fedworld.gov. NTIS is located at 5285 Port Royal Road, Springfield, VA, 22161, USA.
NTIS Prices: PC A10/MF A02
... central heating furnaces--was reviewed. Advanced in technology achieved since the mid-1980s were the **primary** focus. **Key** findings of the review included: (1) the new source performance standard (NSPS) **certification** procedure only qualitatively predicts the level of emissions from wood heaters under actual use in...

... noncertified woodstoves); (4) new technology appliances and fuels can reduce emissions significantly; (5) the International **Organizatin** for Standardization and EPA NSPS test procedures are quite dissimilar, and data generated by the **two** procedures would not be comparable; and (6) the effect of wood moisture and wood type...

18/3,K/11 (Item 2 from file: 6)
DIALOG(R)File 6:NTIS

2116883 NTIS Accession Number: PB99-122111/XAB
Residential Wood Combustion Technology Review. Volume 1. Technical Report
(Final rept. Jul 97-Jul 98)
Houck, J. E. ; Tiegs, P. E.
OMNI Environmental Services, Inc., Beaverton, OR.
Corp. Source Codes: 089645000
Sponsor: Environmental Protection Agency, Research Triangle Park, NC. Air Pollution Prevention and Control Div.
Report No.: EPA/600/R-98/174A
Dec 1998 44p
Languages: English
Journal Announcement: GRAI9911
See also Volume 2, PB99-122129. Sponsored by Environmental Protection Agency, Research Triangle Park, NC. Air Pollution Prevention and Control Div.
Product reproduced from digital image. Order this product from NTIS by: phone at 1-800-553-NTIS (U.S. customers); (703)605-6000 (other countries); fax at (703)605-6900; and email at orders@ntis.fedworld.gov. NTIS is located at 5285 Port Royal Road, Springfield, VA, 22161, USA.
NTIS Prices: PC A04/MF A01
... central heating furnaces--was reviewed. Advanced in technology achieved since the mid-1980s were the **primary** focus. **Key** findings of the review included: (1) the new source performance standard (NSPS) **certification** procedure only qualitatively predicts the level of emissions from wood heaters under actual use in...

... noncertified woodstoves); (4) new technology appliances and fuels can reduce emissions significantly; (5) the International **Organizatin** for Standardization and EPA NSPS test procedures are quite dissimilar, and data generated by the two procedures would not be comparable; and (6) the effect of wood moisture and wood type...

18/3,K/12 (Item 1 from file: 144)
DIALOG(R)File 144:Pascal

12789893 PASCAL No.: 97-0001350
1-V multithreshold-voltage CMOS digital signal processor for mobile phone application
MUTOH S I; SHIGEMATSU S; MATSUYA Y; FUKUDA H; KANEKO T; YAMADA J
NTT System Electronics Lab, Kanagawa, Japan
Proceedings of the 1996 International Solid-State Circuits Conference, ISSCC (San Francisco, CA, USA) 1996-02-08/1996-02-10
Journal: IEEE Journal of Solid-State Circuits, **1996** , 31 (11) 1795-1802
Language: English

1996
A 1-V **power** supply low- **power** and high-speed 16-b fixed-point digital signal processor using a 0.5- mu...

...both high-threshold-voltage and low-threshold-voltage transistors is one key to attaining low **power** consumption with keeping processing throughput high. A maximum operating frequency of 13.2 MHz and an energy consumption of 2.2 mW/MHz were achieved at 1 V. The **second key** to low- **power** operation is a **power** management scheme that uses a secondary embedded microprocessor. This proposed scheme minimizes the standby **power** in the waiting state by effectively controlling the sleep mode in the MTCMOS design. We confirmed that the standby leakage current was reduced three orders of magnitude and that the energy...

... that consumed by conventional CMOS circuits with lowered supply voltage and threshold voltage but without **power** management.

English Descriptors: Digital signal processor; Mobile phone applications;

Threshold voltage; **Power** management scheme; **Power** consumption; Theory ; CMOS integrated circuits; Mobile telecommunication systems; Electric **power** supplies to apparatus; Microprocessor chips; Transistors; Leakage currents; Digital signal processing

...French Descriptors: Circuit integre CMOS; Systeme radiocommunication mobile; Alimentation electrique appareil; Puce microprocesseur; Transistor; Courant fuite; Traitement **numerique** signal

?

22/3,K/1 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC

7256230 INSPEC Abstract Number: B2002-06-6120D-018, C2002-06-6130S-034
Title: An authorization model for a public key management service
Author(s): Samarati, P.; Reiter, M.K.; Jajoidia, S.
Author Affiliation: Milan Univ., Italy
Journal: ACM Transactions on Information and Systems Security vol.4, no.4 p.453-82
Publisher: ACM,
Publication Date: Nov. 2001 Country of Publication: USA
CODEN: ATISBQ ISSN: 1094-9224
SICI: 1094-9224(200111)4:4L.453:AMPM;1-U
Material Identity Number: D380-2002-003
U.S. Copyright Clearance Center Code: 1094-9224/01/1100-0453$5.00
Language: English
Subfile: B C

Abstract: Public key management has received **considerable** attention from both the research and commercial communities as a useful primitive for secure electronic commerce and secure communication. While the mechanics of **certifying** and revoking public keys and escrowing and recovering **private keys** have been widely explored, less attention has been paid to access control frameworks for regulating...

... framework for a key management service that supports public key registration, lookup, and revocation, and **private key** escrow, protected use (e.g., to **decrypt** selected messages), and recovery. We propose an access control model using a policy based on principal, ownership, and **authority** relationships on keys. The model allows owners to grant to others (and revoke) privileges to...
...Descriptors: public key **cryptography** ;

22/3,K/2 (Item 2 from file: 2)
DIALOG(R)File 2:INSPEC

6732254 INSPEC Abstract Number: B2000-11-6120D-032, C2000-11-6130S-043
Title: Ticket and challenge-based protocols for timestamping
Author(s): Peyravian, M.; Matyas, S.M.; Roginsky, A.; Zunic, N.
Author Affiliation: IBM Corp., Research Triangle Park, NC, USA
Journal: Computers & Security vol.19, no.6 p.551-8
Publisher: Elsevier,
Publication Date: 2000 Country of Publication: UK
CODEN: CPSEDU ISSN: 0167-4048
SICI: 0167-4048(2000)19:6L.551:TCBP;1-N
Material Identity Number: M680-2000-006
U.S. Copyright Clearance Center Code: 0167-4048/2000/$20.00
Language: English
Subfile: B C

Abstract: We introduce **two** methods that allow you to **certify** the time when a particular document was presented to a **certifying authority** . While some of the algorithms that served this purpose already existed in the literature, our methodology has significant practical advantages. The **two** methods we show are more straightforward, by giving a user a chance, in some cases, to operate on one value rather than **two** . They give the user the flexibility to select the most appropriate algorithm. They provide for a reasonable sharing of the workload between the user and the timestamping **authority** .
Descriptors: **cryptography** ;
...Identifiers: **certifying authority** ; ...

...public key **cryptography** ; ...

... **private key cryptography**

22/3,K/3 (Item 1 from file: 6)
DIALOG(R)File 6:NTIS
(c) 2002 NTIS, Intl Cpyrght All Rights Res. All rts. reserv.

2204667 NTIS Accession Number: ADP010879/XAB
Design Aspects in a Public Key Infrastructure for Network Applications Security
Patriciu, V. V. ; Serb, A.
Military Technical Academy, Bucharest (Romania). Computer Engineering Dept.
Corp. Source Codes: 118096001; 439348
Apr 2000 12p
Languages: English Document Type: Conference proceeding; Journal article
Journal Announcement: USGRDR0123
Original document contains color images. Pres. at RTO information Systems Technology Panel (IST), Istanbul, Turkey 9-11 Oct 2000. This article is from ADA391919 New Information Processing Techniques for Military Systems (les Nouvelles techniques de traitement de l'information pour les systemes militaires) p14-1/14-12.
Product reproduced from digital image. Order this product from NTIS by: phone at 1-800-553-NTIS (U.S. customers); (703)605-6000 (other countries); fax at (703)605-6900; and email at orders@ntis.gov. NTIS is located at 5285 Port Royal Road, Springfield, VA, 22161, USA.
NTIS Prices: PC A03/MF A01
... This paper will concentrate on an interesting area of software security based on public key **cryptographic** technology. The Public Key system makes it possible for **two** parties to communicate securely without either having to know or trust the other party. This is possible because a third party that both the other parties trust identifies them and **certifies** that their keys are genuine. This third party is called the **Certification Authority** , or CA. CA guarantees that they are who they claim to be. The CA does this by registering each user's identification information and issuing them with a set of **Private keys** and a set of Public Key Certificates. A worldwide Public Key Infrastructure (PKI) that supports...

...and state policies/regulations will not be available in the near future. In the meantime **organizations** and corporations can utilize this security technology to satisfy current business needs. **Many organizations** are choosing to manage their own Certificate **Authority** (CA) instead of outsourcing this function to a third party (i.e. Verisign, Thawte, GTE...
Descriptors: Meetings; * **Cryptography** ; *Computer access control; Information systems; Identification; Computer networks; Information security; Reprints
Identifiers: Component report; Foreign reports; Nato furnished; Pki(Public key infrastructure); **Encryption** ; NTISDODXR

22/3,K/4 (Item 1 from file: 144)
DIALOG(R)File 144:Pascal
(c) 2002 INIST/CNRS. All rts. reserv.

15579524 PASCAL No.: 02-0280332
Co-operatively formed group signatures
Topics in cryptology - **CT-RSA 2002 : San Jose CA, 18-22 February 2002**
MAITLAND Greg; BOYD Colin
PRENEEL Bart, ed
Information Security Research Centre, Queensland University of Technology , Brisbane, Australia
The cryptographers' track. Conference (San Jose CA USA) 2002-02-18
Journal: Lecture notes in computer science, 2002, 2271 218-235
Language: English

Co-operatively formed group **signatures**
Topics in cryptology - **CT-RSA 2002 : San Jose CA, 18-22 February 2002**
Group signatures and their applications have received **considerable** attention in the literature in recent times. Substantial gains have been made with respect to designing provably secure and efficient schemes. In practice, as with all signature schemes, deploying **group** signature schemes requires the **group** member's signing keys to be both physically and electronically secure from theft. Smartcards or...
... offered as a solution to this problem. We consider the possibility of co-operatively forming **group** signatures so as to balance the processing load between a modestly performed secure device and a much more **powerful** workstation. The constructions are based on the observation that **several** recent **group** signature schemes have adopted a structure which utilises **two** values in signature creation - a **private** signing **key** and a **group** membership certificate. We describe a co-operative **group** signature scheme based on a recently proposed scheme as well as a 'wallet with observer...

English Descriptors: **Certification** ; Smart cards; Theft protection; **Cryptography** ; Digital signature

French Descriptors: **Certification** ; Carte a puce; Protection vol; **Cryptographie** ; Signature **numerique** ; Signature **groupe**

Spanish Descriptors: Certificacion; Proteccion robos; Criptografia; Firma **numerica**

22/3,K/5 (Item 2 from file: 144)
DIALOG(R)File 144:Pascal

15459704 PASCAL No.: 02-0152957
Defense and security of a wireless tactical network
Digital wireless communication III : Orlando FL, 17-18 April 2001
YOUNGER Michael; YOUNG Stuart
RAO Raghuveer M, ed; DIANAT Soheil A, ed; ZOLTOWSKI Michael D, ed
U. S. Army Research Labs, 2800 Powder Mill Road, Adelphi, MD 20783, Jamaica
International Society for Optical Engineering, Bellingham WA, United States
Digital wireless communication. Conference, 3 (Orlando FL USA) 2001-04-17
Journal: SPIE proceedings series, 2001, 4395 224-232
Language: English

... resources, and expertise to safeguard a host are only some of the reasons that so **many** systems are insecure any type of network commercial or tactical. To compound the problem, like...

... on (simply due to usage), but with the rapidly changing security field, it also requires **considerable** effort to stay abreast of the latest information. Army Research Labs (ARL) is trying to...

... ARL will determine what works and how they work in the tactical area. There are **numerous** ways to protect the wire/wireless network via public domain or commercial software. Some of...

... bandwidth, complexity, implementation and deployment of monitoring and auditing tools. The implementation and deployment of **encryption** , public and **private** **key** information, and certificate **authority** . Also, ARL will address configuration problems, correcting or catching misuse and misunderstandings, and computers that...

English Descriptors: Computer security; Wireless telecommunication; Telecommunication network; Operating system; Expertise; Monitoring; Software; Passband; Implementation; **Cryptography** ; Public key; Public

information; **Private key** ; **Certification** ; Signal processing; **Encryption**

French Descriptors: Securite informatique; Telecommunication sans fil; Reseau telecommunication; Systeme exploitation; Expertise; Monitorage; Logiciel; Bande passante; Implementation; **Cryptographie** ; Cle publique; Information public; Cle privee; **Certification** ; Traitement signal; Chiffrement

?

```
Set     Items   Description
S1          0   AU= (CORDERY R? OR CORDERY, R?)
S2         27   CERTICOM
S3         12   ELLIPTIC(2N)CURV? OR HYPERELLIPTIC(2N)CURV?
S4        557   (PRIVAT? OR PUBLIC? OR SECRET? OR FIRST OR SECOND? OR PRIM-
              AR?)(1W) KEY? ?
S5      10626   HCC OR AVC OR CODIF? OR DECOD? OR UNENCOD? OR DECRYPT? OR -
              UNENCRYPT? OR UNCRYPT? OR CIPHER? OR CYPHER? OR ENCOD? OR COD-
              E? ? OR CODING? OR ENCOD? OR ENCIPHER? OR ENCYPHER? OR UNCOD?
              OR DECIPHER? OR DECYPHER? OR UNENCIPHER? OR UNENCYPHER?
S6       2347   UNCIPHER? OR UNCYPHER? OR CRYPTO? OR ENCRYPT?
S7       1052   (CERTIFYING? OR CERTIFY OR CERTIFICATION? OR CERTIFIES OR -
              CONFIRM? OR VERIFY? OR ATTEST?)(2N)(STATION? OR AUTHORIT? OR -
              POWER? OR AGENC? OR ORGANI? OR BOARD?) OR CA
S8      56563   MULTI? OR PLURAL? OR MANY OR SEVERAL? OR NUMER? OR CLUSTER?
               OR GROUP? OR MULTIPL? OR PLENTY? OR CONSIDERABLE? OR TWO OR -
              DUAL OR DOUBL?
S9         43   S4 AND (S5 OR S6) AND S7
S10         5   S4(10N)(S5 OR S6)(10N)S7
S11         8   S2 AND S3
S12         3   (S8(2N)S7) AND S4
?show files
File 256:SoftBase:Reviews,Companies&Prods. 82-2002/Jul
         (c)2002 Info.Sources Inc
?
```

10/3,K/1
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00122162 DOCUMENT TYPE: Review

PRODUCT NAMES: Extranets (837385); Digital Certificates (840271)

TITLE: The Security Behind Secure Extranets
AUTHOR: Paget, Paul
SOURCE: Enterprise Systems Journal, v14 n12 p74(4) Dec 1999
ISSN: 1053-6566
HOMEPAGE: http://www.esj.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

REVISION DATE: 20000430

...through a digital audit trail. Public key infrastructure (PKI), which is based on public key **cryptography** , also secures transactions over the Internet by using public and private components. Messages transported are **encrypted** with a **public key** and are then read by the receiver with a **private key** . Other superior security methods for extranets described are trusted parties (**certification authorities**) and registration authorities.

10/3,K/2
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00118558 DOCUMENT TYPE: Review

PRODUCT NAMES: Jasmine TND (770639); CA-Unicenter TND (693529); PLATINUM ADvantage TND (710571); DecisionBase TND (741833); ERwin (331627)

TITLE: CA Emphasizes Jasmine Database
AUTHOR: Whiting, Rick Davis, Beth
SOURCE: Information Week, v745 p26(1) Jul 26, 1999
ISSN: 8750-6874
HOMEPAGE: http://www.informationweek.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

REVISION DATE: 20020321

...included. The ManageIT data management suite will meld PLATINUM Enterprise DBA and DBVision with the **CA** -Datacom management tool. The new eTrust product line will include single sign-on, security, **encryption** , firewall software, **public - key** infrastructure technology, and other e-commerce tools. At **CA** World, **CA** handed out thousands of developer's kits for Jasmine TND, which is an upgrade to...

10/3,K/3
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00110800 DOCUMENT TYPE: Review

PRODUCT NAMES: Encryption (832022)

TITLE: PKI tames network security
AUTHOR: McClure, Stuart
SOURCE: InfoWorld, v20 n37 p65(2) Sep 14, 1998

ISSN: 0199-6649
HOMEPAGE: http://www.infoworld.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

REVISION DATE: 20020630

...bring a higher level of flexibility. A PKI has several components which work together to **encrypt** data and create digital certificates. On the back end, a database manages digital certificates and public and **private keys** . The certificate authority (**CA**) signs each digital certificate before sending it to the requesting client. After a certificate is created, it is stored in an X.500 directory. The **CA** creates two pairs of public and **private keys** for each user or server; one pair is used for **encrypting** and **decrypting** information, and the other is used by client applications to create a digital signature on...

10/3,K/4
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.
(c)2002 Info.Sources Inc. All rts. reserv.

00104232 DOCUMENT TYPE: Review

PRODUCT NAMES: Pretty Good Privacy (835072)

TITLE: Breaking The Code For Network Security
AUTHOR: Delmonico, Dayna
SOURCE: InternetWeek, v686 p75(4) Oct 20, 1997
ISSN: 0746-8121
HOMEPAGE: http://www.internetwk.com

RECORD TYPE: Review
REVIEW TYPE: Product Comparison
GRADE: Product Comparison, No Rating

REVISION DATE: 20000228

...With private key encryption, only the sender and receiver know the key. With public key **encryption** , senders and receivers hold a common key and some get an additional **private key** . When **encryption** is required for multiple users, a Certificate Authority (**CA**) is required. One of the most popular **encryption** schemes is the Data Encryption Standard (DES). DES allows the receiver and sender to use...

10/3,K/5
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.
(c)2002 Info.Sources Inc. All rts. reserv.

00100882 DOCUMENT TYPE: Review

PRODUCT NAMES: e-Lock (657859); Netscape Certificate Server 1.0 (650455) ; SENTRY CA (657841); Microsoft Internet Explorer (577375)

TITLE: CAs (Certificate Authorities): How Valuable Are They?
AUTHOR: Shipley, Greg
SOURCE: Network Computing, v8 n6 p54(10) Apr 1, 1997
ISSN: 1046-4468
HOMEPAGE: http://www.NetworkComputing.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

REVISION DATE: 20000228

...Windows-based client that supports secure multipurpose mail extension (S/MIME), a protocol that uses **public key encryption** over e-mail, improving security. Microsoft's Microsoft Internet Explorer 3.01 also includes a **CA** program feature that is not yet up and running. Smarty from Fisher International is a...
?

11/3,K/1
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

02661333 DOCUMENT TYPE: Company

Certicom **Corp (661333**
25821 Industrial Blvd #300
Hayward, CA 94545 United States
TELEPHONE: (510) 780-5400
FAX: (510) 780-5401
HOMEPAGE: http://www.certicom.com
EMAIL: info@certicom.com

RECORD TYPE: Directory

CONTACT: Sales Department

ORGANIZATION TYPE: Corporation
EQUITY TYPE: Public
STATUS: Active

SALES: NA

DATE FOUNDED: 1985
PERSONNEL: Williams, Robert L, VP Operations; Panjwani, Prakash, VP Sales; Panjwani, Prakash, VP Business Development; Capitolo, Gregory, VP Finance; Capitolo, Gregory, Chief Financial Officer; Charlebois, Dr Dennis J, VP; Dierks, Tim, Chief Technology Officer
REVISION DATE: 20020416

Certicom **Corp...**

company uses its **Elliptic Curve** Cryptography (ECC) for its encryption technology. Partners and customers include Symbian, H&R Block, Sun...

11/3,K/2
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

01084263 DOCUMENT TYPE: Product

PRODUCT NAME: MobileTrust Server Certificates (084263)

Certicom Corp (661333
25821 Industrial Blvd #300
Hayward, CA 94545 United States
TELEPHONE: (510) 780-5400

RECORD TYPE: Directory

CONTACT: Sales Department

REVISION DATE: 020625

Certicom Corp...

MobileTrust (TM) Server Certificates from **Certicom** are the basis for ensuring trust on the Internet, where communications pass blindly from computer...

...identity of the computer they are communicating with. These are accepted by applications built with **Certicom** SSL Plus and WTLS Plus toolkits; they also interoperate with most RSA server applications. Certificates...

...only Certificate Authority (CA) to offer standards-based server certificates that employ both RSA and **elliptic curve** cryptography (ECC) algorithms, which secure communications in both wireline and wireless

environments. Its data centers...

11/3,K/3
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.
(c)2002 Info.Sources Inc. All rts. reserv.

01084255 DOCUMENT TYPE: Product

PRODUCT NAME: WTLS Plus 1.1 (084255)

Certicom Corp (661333
25821 Industrial Blvd #300
Hayward, CA 94545 United States
TELEPHONE: (510) 780-5400

RECORD TYPE: Directory

CONTACT: Sales Department

REVISION DATE: 020521

Certicom Corp...

WTLS Plus (TM) from **Certicom** is a WTLS toolkit that offers full strength WTLS security. WTLS is a WAP Forum standard that is ideally suited for WAP implementations. It taps ECC (**elliptic curve** cryptography) technology, which can support client authentication on any embedded device. This wireless security solution...

11/3,K/4
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.
(c)2002 Info.Sources Inc. All rts. reserv.

01084247 DOCUMENT TYPE: Product

PRODUCT NAME: SSL Plus (084247)

Certicom Corp (661333
25821 Industrial Blvd #300
Hayward, CA 94545 United States
TELEPHONE: (510) 780-5400

RECORD TYPE: Directory

CONTACT: Sales Department

REVISION DATE: 020625

Certicom Corp...

SSL Plus (TM) from **Certicom** is the industry's most widely deployed commercial Secure Sockets Layer (SSL) product. It offers ease of use, rapid development, and support for RSA, DSA/Diffie-Helman, and **elliptic curve** cryptography (ECC)--the only SSL product with that capability. The toolkit supports a wide range...

11/3,K/5
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.
(c)2002 Info.Sources Inc. All rts. reserv.

01084191 DOCUMENT TYPE: Product

PRODUCT NAME: Security Builder (084191)

Certicom Corp (661333
25821 Industrial Blvd #300

Hayward, CA 94545 United States
TELEPHONE: (510) 780-5400

RECORD TYPE: Directory

CONTACT: Sales Department

REVISION DATE: 020521

Certicom Corp...

Certicom 's Security Builder is a cryptographic toolkit that allows developers to add signatures, key management, and encryption to applications. Security Builder uses **elliptic curve** cryptography (ECC) technology to create solid, scalable security features for a wide range of computing...

11/3,K/6
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

01038113 DOCUMENT TYPE: Product

PRODUCT NAME: movianVPN 2.1 (038113)

Certicom Corp (661333
25821 Industrial Blvd #300
Hayward, CA 94545 United States
TELEPHONE: (510) 780-5400

RECORD TYPE: Directory

CONTACT: Sales Department

REVISION DATE: 020424

Certicom Corp...

movianVPN 2.1 from **Certicom** is an award-winning software VPN client that supports the leading VPN security standard IPSec...

...supports popular devices that run Palm OS or Windows CE. Other features of movianVPN include **Elliptic Curve** Crytpography (ECC) and a small memory footprint.

11/3,K/7
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00138486 DOCUMENT TYPE: Review

PRODUCT NAMES: PKI (838896); Trustpoint Certificate Authority (099571)

TITLE: Bite-sized keys lock aeronautical network: Elliptic curve ...
AUTHOR: Frank, Diane
SOURCE: Federal Computer Week, v16 n11 p28(1) Apr 15, 2002
ISSN: 0893-052X
HOMEPAGE: http://www.fcw.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

REVISION DATE: 20020730

TITLE: Bite-sized keys lock aeronautical network: Elliptic curve ...

The Federal Aviation Administration (FAA) chose **Certicom** 's Trustpoint Certificate Authority public key infrastructure (PKI) to secure air-to-ground data communications...
...s digital certificate and encryption technology offer the foundations of PKI and are based on **elliptic curve** cryptography (ECC). ECC creates encryption keys that require a great deal less bandwidth than other...

...COMPANY NAME: 999999); **Certicom** Corp...

11/3,K/8
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00128120 DOCUMENT TYPE: Review

PRODUCT NAMES: Bluetooth (841455); WAP (839027); Palm.Net (030163); Elliptic Curve **Cryptography (030171); BlackBerry (755818**

TITLE: The LAN, PAN, WAN Plan: Wireless technologies can plug in mobile...
AUTHOR: Brooks, Jason Bethoney, Herb
SOURCE: eWeek, v18 n2 p48(2) Jan 15, 2001
ISSN: 1530-6283
HOMEPAGE: http://www.eweek.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

REVISION DATE: 20020228

...PRODUCT NAMES: 030163); Elliptic Curve **Cryptography...**

Bluetooth SIG's Bluetooth, Wireless Application Protocol (WAP), Palm's Palm.Net, **Certicom** 's **Elliptic Curve** Cryptography, and Research in Motion's Blackberry are highlighted in a discussion of wireless technologies...

...COMPANY NAME: 528943); **Certicom** Corp...
?

12/3,K/1
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

01081469 DOCUMENT TYPE: Product

PRODUCT NAME: SSH Certifier PKI Product Family (081469)

SSH Communications Security Inc (698083)
1076 E Meadow Cir
Palo Alto, CA 94303 United States
TELEPHONE: (650) 251-2700

RECORD TYPE: Directory

CONTACT: Sales Department

REVISION DATE: 020625

...SSH Certifier PKI Product Family targets service providers and companies looking for scalable, X.509 **public key** infrastructure (PKI) systems. SSH Certifier PKI Product Family encompasses the SSH Certifier (TM), which offers...

...PKI technology across growing networks. The application offers online certificate enrollment, publication of certificates to **multiple** directories, unlimited **Certification Authorities** (CAs), and other features. The SSH Token Master provides a streamlined interface that allows nontechnical...

12/3,K/2
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00138337 DOCUMENT TYPE: Review

PRODUCT NAMES: Company--Computer Associates International Inc (850161)

TITLE: CA's new reorg keys on security: Vendor regrouping as five brand...
AUTHOR: Fisher, Dennis
SOURCE: eWeek, v19 n17 p1(2) Apr 29, 2002
ISSN: 1530-6283
HOMEPAGE: http://www.eweek.com

RECORD TYPE: Review
REVIEW TYPE: Company

REVISION DATE: 20020730

...security standards rely substantially on the identity of IBM, Entrust, and RSA. CA has a **public key** infrastructure (PKI) and access management products, but IBM, Entrust, and RSA Security have very large markets and **considerable** experience. **CA** has decided to position its products in five brand units, and each will have its...

12/3,K/3
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00110800 DOCUMENT TYPE: Review

PRODUCT NAMES: Encryption (832022)

TITLE: PKI tames network security
AUTHOR: McClure, Stuart
SOURCE: InfoWorld, v20 n37 p65(2) Sep 14, 1998
ISSN: 0199-6649

HOMEPAGE: http://www.infoworld.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

REVISION DATE: 20020630

...be managed separately. One way to take control over the security environment is through a **public key** infrastructure (PKI). The PKI accommodates data encryption and digital signatures through a certificate-based framework...
...create digital certificates. On the back end, a database manages digital certificates and public and **private keys** . The certificate authority (CA) signs each digital certificate before sending it to the requesting client. After a certificate is created, it is stored in an X.500 directory. The **CA** creates **two** pairs of public and **private keys** for each user or server; one pair is used for encrypting and decrypting information, and
...
?

Set	Items	Description
S1	64	AU= (CORDERY R? OR CORDERY, R?)
S2	14	CERTICOM
S3	4617	ELLIPTIC(2N)CURV? OR HYPERELLIPTIC(2N)CURV?
S4	13976	(PRIVAT? OR PUBLIC? OR SECRET? OR FIRST OR SECOND? OR PRIMAR?)(1W) KEY? ?
S5	1177994	HCC OR AVC OR CODIF? OR DECOD? OR UNENCOD? OR DECRYPT? OR UNENCRYPT? OR UNCRYPT? OR CIPHER? OR CYPHER? OR ENCOD? OR CODE? ? OR CODING? OR ENCOD? OR ENCIPHER? OR ENCYPHER? OR UNCOD? OR DECIPHER? OR DECYPHER? OR UNENCIPHER? OR UNENCYPHER?
S6	114235	UNCIPHER? OR UNCYPHER? OR CRYPTO? OR ENCRYPT?
S7	525215	(CERTIFYING? OR CERTIFY OR CERTIFICATION? OR CERTIFIES OR CONFIRM? OR VERIFY? OR ATTEST?)(2N)(STATION? OR AUTHORIT? OR POWER? OR AGENC? OR ORGANI? OR BOARD?) OR CA
S8	16006517	MULTI? OR PLURAL? OR MANY OR SEVERAL? OR NUMER? OR CLUSTER? OR GROUP? OR MULTIPL? OR PLENTY? OR CONSIDERABLE? OR TWO OR DUAL OR DOUBL?
S9	442	S4 AND (S5 OR S6) AND S7
S10	34	S4(3N)(S5 OR S6)(3N)S7
S11	29	RD (unique items)
S12	22	S11 AND PY<=1999
S13	19	(S8(2N)S7) AND S4
S14	13	RD (unique items)
S15	7	S14 AND PY<=1999
S16	7	S15 NOT S12

```
? show files
File 238:Abs. in New Tech & Eng. 1981-2002/Jul
         (c) 2002 Cambridge Scient. Abstr
File   8:Ei Compendex(R) 1970-2002/Aug W2
         (c) 2002 Engineering Info. Inc.
File  77:Conference Papers Index 1973-2002/Jul
         (c) 2002 Cambridge Sci Abs
File  35:Dissertation Abs Online 1861-2002/Jul
         (c) 2002 ProQuest Info&Learning
File 202:Information Science Abs. 1966-2002/Jul 03
         (c) Information Today, Inc
File   2:INSPEC 1969-2002/Aug W2
         (c) 2002 Institution of Electrical Engineers
File 233:Internet & Personal Comp. Abs. 1981-2002/Aug
         (c) 2002 Info. Today Inc.
File  94:JICST-EPlus 1985-2002/Jun W3
         (c)2002 Japan Science and Tech Corp(JST)
File   6:NTIS 1964-2002/Aug W4
         (c) 2002 NTIS, Intl Cpyrght All Rights Res
File 144:Pascal 1973-2002/Aug W2
         (c) 2002 INIST/CNRS
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File  62:SPIN(R) 1975-2002/Jul W2
         (c) 2002 American Institute of Physics
File  99:Wilson Appl. Sci & Tech Abs 1983-2002/Jun
         (c) 2002 The HW Wilson Co.
File  34:SciSearch(R) Cited Ref Sci 1990-2002/Aug W2
         (c) 2002 Inst for Sci Info
```

12/3,K/1 (Item 1 from file: 238)
DIALOG(R)File 238:Abs. in New Tech & Eng.

0319909 ANTE NUMBER: 83769
Signing away the future
AUTHOR(S): Harrington, T.
JOURNAL: Computing 11 Mar 1999 p.53-4, 56.
PUBLICATION YEAR: **1999**
ISSN: 0144-3097
BLDSC SHELF MARK: 3395.009
LANGUAGE: English

PUBLICATION YEAR: **1999**

ABSTRACT: ...with regard to digital signatures for online transactions is examined. Problems in the UK with **encryption** , **public / private key cryptography** , and **certifying authorities** (trusted third parties) are discussed, and compared to the situation in other European countries and...

12/3,K/2 (Item 1 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

05083380 E.I. No: EIP98084311704
Title: Evaluating certification authority security
Author: Kent, Stephen
Corporate Source: BBN Technologies, Cambridge, MA, USA
Conference Title: Proceedings of the 1998 IEEE Aerospace Conference. Part 4 (of 5)
Conference Location: Snowmass at Aspen, CO, USA Conference Date: 19980321-19980328
E.I. Conference No.: 48731
Source: IEEE Aerospace Applications Conference Proceedings v 4 1998. IEEE Comp Soc, Los Alamitos, CA, USA,98TH8339. p 319-327
Publication Year: 1998
CODEN: 85OMAZ
Language: English

Identifiers: **Certification Authorities (CA); Public key cryptography** (PKC)

12/3,K/3 (Item 2 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

04665354 E.I. No: EIP97043595398
Title: Inferno security
Author: Presotto, David Leo
Corporate Source: Bell Labs
Conference Title: Proceedings of the 1997 IEEE COMPCON Conference
Conference Location: San Jose, CA, USA Conference Date: 19970223-19970226
E.I. Conference No.: 46226
Source: Digest of Papers - COMPCON - IEEE Computer Society International Conference 1997. IEEE, Piscataway, NJ, USA,97CB36028. p 251-253
Publication Year: 1997
CODEN: DCSIDU
Language: English

...Abstract: encryption, message digesting, and digital signatures. Authentication and digital signatures are performed using public key **cryptography** . **Public keys** are certified by Inferno-based **certifying authorities** that sign the **public keys** with their own private key. (Author abstract) 7 Refs.

12/3,K/4 (Item 3 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

03843554 E.I. No: EIP94041269137
Title: Privacy enhanced mail in more detail
Author: Zegwaart, Erik
Corporate Source: SURFnet bv, Utrecht, Neth
Source: Computer Networks and ISDN Systems v 25 n SUPPL 2 1993. p S63-S71
Publication Year: 1993
CODEN: CNETDP ISSN: 0169-7552
Language: English

Identifiers: Privacy enhanced mail; **Public key cryptology** ; **Certification authority**

12/3,K/5 (Item 4 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

03571839 E.I. Monthly No: EIM9303-011952
Title: COSINE sub-project P8: security services.
Author: Purser, Michael
Corporate Source: Baltimore Technologies Ltd, Dublin, Ireland
Conference Title: 3rd Joint European Networking Conference
Conference Location: Innsbruck, Austria Conference Date: 19920511
E.I. Conference No.: 17547
Source: Computer Networks and ISDN Systems v 25 n 4-5 Nov 1992. p 476-482
Publication Year: 1992
CODEN: CNISE9 ISSN: 0169-7552
Language: English

...Abstract: limited but attainable goals of secure E-Mail and secure remote access, supported by a **Certification Authority** and **public key cryptographic** functions, is intended to demonstrate that these functions can be provided in a relatively short...

12/3,K/6 (Item 1 from file: 35)
DIALOG(R)File 35:Dissertation Abs Online

01431139 ORDER NO: AADAA-I9527269
A COMMON APPROACH TO EXTENDING COMPUTER SECURITY CONCEPTS TO THE UNIVERSAL DISTRIBUTED NON-TRUSTED ENVIRONMENT (INFORMATION PROTECTION, ACCESS CONTROL)
Author: HERSCHAFT, RICHARD DAN
Degree: D.ENG.
Year: **1994**
Corporate Source/Institution: SOUTHERN METHODIST UNIVERSITY (0210)
Source: VOLUME 56/05-B OF DISSERTATION ABSTRACTS INTERNATIONAL. PAGE 2781. 174 PAGES

Year: **1994**

...extended to work in this environment are the security watchdog, the access control list, and **public key cryptography** with its **certification authority** . Also developed are the concepts of a tamper proof device, a device validation authority, and...

12/3,K/7 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC

6137991 INSPEC Abstract Number: B1999-02-6120D-050, C1999-02-6130S-070
Title: Key management unit CK-Guard

Author(s): Hosokawa, T.; Miyauchi, H.; Kimura, M.
Author Affiliation: Data Commun. Div., NEC Corp., Japan
Journal: NEC Technical Journal vol.51, no.9 p.146-9
Publisher: NEC,
Publication Date: Sept. 1998 Country of Publication: Japan
CODEN: NECGEZ ISSN: 0285-4139
SICI: 0285-4139(199809)51:9L.146:MUG;1-P
Material Identity Number: H719-1998-012
Language: Japanese
Subfile: B C

...Abstract: private keys is a crucial issue in systems which require high-level security, such as **certification authorities** based on the RSA **public key cryptosystem** . NEC has developed tamper resistant private key management equipment, CK-Guard. CK-Guard is accessed...
1998

12/3,K/8 (Item 2 from file: 2)
DIALOG(R)File 2:INSPEC

6029201 INSPEC Abstract Number: C9811-6130S-009
Title: Chip cards for secure transactions over the Internet
Author(s): Heins, K.; Luke, G.
Journal: Elektronik vol.47, no.12 p.74-9
Publisher: Franzis-Verlag,
Publication Date: 9 June 1998 Country of Publication: Germany
CODEN: EKRKAR ISSN: 0013-5658
SICI: 0013-5658(19980609)47:12L.74:CCST;1-0
Material Identity Number: E071-98013
Language: German
Subfile: C

...Abstract: can verify signatures, is described. The authors refer to the asymmetrical RSA security process, including **encryption** and signature validation. **Public key CA** is discussed and the SmartOS operating system for chip cards is described.
1998

12/3,K/9 (Item 3 from file: 2)
DIALOG(R)File 2:INSPEC

4906923 INSPEC Abstract Number: B9505-6120B-003, C9505-6130S-003
Title: Issues in using public-key cryptography in signing electronic documents
Author(s): Wright, B.
Journal: EDPACS vol.22, no.9 p.9-12
Publication Date: March 1995 Country of Publication: USA
CODEN: EDPCDF ISSN: 0736-6981
Language: English
Subfile: B C

...Abstract: costs something; (iii) standards are necessary; and (iv) public keys are hard to manage. When **public - key cryptography** employing a **certification authority** is used to sign a legal document, the parties to the transaction are seeking to...
1995

12/3,K/10 (Item 4 from file: 2)
DIALOG(R)File 2:INSPEC

4672570
Title: The role of the trusted third party
Journal: Financial Technology Insight p.17-18
Publication Date: April 1994 Country of Publication: UK
CODEN: FTINEZ ISSN: 0961-5342
U.S. Copyright Clearance Center Code: 0961-5342/94/$7.00
Language: English
Subfile: D

...Abstract: parties may act as TTPs for specific functions, the most obvious example here being the **certification authority** for **public encryption keys** . This function is defined under the CCITT recommendations for directory services X.509. This TTP...
1994

12/3,K/11 (Item 5 from file: 2)
DIALOG(R)File 2:INSPEC

03513835 INSPEC Abstract Number: B89077146, C90002792
Title: TeleTrusT-OSIS overview
Author(s): Rihaczek, K.
Conference Title: Research into Networks and Distributed Applications. European Teleinformatics Conference - EUTECO '88 p.443-53
Editor(s): Speth, R.
Publisher: North-Holland, Amsterdam, Netherlands
Publication Date: 1988 Country of Publication: Netherlands xix+1237 pp.
ISBN: 0 444 70428 0
Conference Date: 20-22 April 1988 Conference Location: Vienna, Austria
Language: English
Subfile: B C

...Abstract: signature mechanism and a trusted third party are needed. Such signatures can be affected using **public key** data **encryption** . The trusted third party, a **certification authority** , distributes individual pairs of keys and verification keys' certificates.
1988

12/3,K/12 (Item 1 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00543590 99IW08-103
Sorting out security -- Early users find digital certificates cost-effective for secure business-to-business authentication
Mendel, Brett
InfoWorld , August 9, 1999 , v21 n32 p32-33, 2 Page(s)
ISSN: 0199-6649

... passwords and firewalls. Explains that PKI uses a system of digital certificates and certificate authorities (**CA**) to authenticate users. Adds that PKI uses public and **private key encryption** to protect data integrity. Indicates that mainstream deployment of PKI has been hampered by factors...
1999

12/3,K/13 (Item 2 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00531099 99SD04-006
Product toolbox
Software Development , April 1, 1999 , v7 n4 ps7, 1 Page(s)
ISSN: 0749-2839
Company Name: RPK Security; ValiCert; Baltimore Technologies; Entrust

Technologies; Centura Software
URL: http://www.rpkusa.com http://www.valicert.com http://www.baltimoreinc.com http://www.entrust.com http://www.centurasoftware.com
Product Name: RPK Encryptonite Software Toolkit; Enterprise VA Suite 2.0; J/CRYPTO; Entrust/PKI Developer Edition; SQLBase 7.5

... tools. Says that the RPK Encryptonite Software Toolkit ($695) from RPK Security of San Francisco, **CA** (212) enables adding **public key** security without significant knowledge of **cryptography** . Adds that Enterprise VA Suite 2.0 ($25,000) from ValiCert Inc. of Mountain View...
1999

12/3,K/14 (Item 3 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00510369 98EA10-010
Confidentiality, authentication, and integrity for e-mail -- PGP for Personal Privacy 5.5.5 and PGP Business Security Suite 5.5 put encryption a click away
Cobb, Michael
e-Business Advisor , October 1, 1998 , v16 n10 p52-55, 3 Page(s)
ISSN: 1098-8912
Company Name: Network Associates
URL: http://www.pgp.com http://www.pgp.com
Product Name: PGP for Personal Privacy 5.5.5; PGP Business Security Suite 5.5

... 5.5 ($109.95), two data encryption solutions from Network Associates Inc. of Santa Clara, **CA** (408). Explains that these products are designed to **encrypt** e-mail and attached files using **public key cryptography** . Notes that PGP for Personal Privacy provides an easy-to-use encryption solution which integrates...
1998

12/3,K/15 (Item 4 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00489223 98WC03-004
Securing your electronic environment -- Keeping files transmitted over the Web secure is a major concern; PGP for Business Security, eSafe Protect Enterprise Edition, and...
Levine, Daniel B
Windows Sources , March 1, 1998 , v6 n3 p130-136, 4 Page(s)
ISSN: 1065-9641
Company Name: Network Associates; eSafe Technologies; Frontier Technologies
URL: http://www.pgp.com http://www.esafe.com http://www.frontiertech.com
Product Name: PGP for Business Security 5.5; Safe Protect Enterprise Edition; e-Lock 2

... software packages. Says PGP for Business Security 5.5 ($119) from Network Associates, San Mateo, **CA** (888) is a mature **public - key cryptography** product that is also easy to use. Adds that the suite includes a certificate server...
1998

12/3,K/16 (Item 5 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00474959 97LA10-108
Privacy better than ``pretty good''
Apicella, Mario

LAN Times , October 13, 1997 , v14 n21 p55, 1 Page(s)
ISSN: 1040-5917
Company Name: Pretty Good Privacy
URL: http://www.pgp.com
Product Name: PGP for Personal Privacy

...32-bit Windows and Macintosh encryption tool from Pretty Good Privacy Inc. of San Mateo, **CA** (888). Says it uses a **public key** associated with the user's e-mail address to **encrypt** data and a **private key** to **decrypt** it. Adds that it facilitates storing the **public key** on a public key server on the Internet which can also be used to verify...
1997

12/3,K/17 (Item 6 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00366904 94NC11-009
The electronic wallet
Curtis, Walt; Schnaidt, Patricia
Network Computing , November 15, 1994 , v5 n14 p56-57, 2 Page(s)
ISSN: 1046-4468

... IPower secure token, a form of digital cash developed by National Semiconductor of Santa Clara, **CA** . Says it incorporates **public key cryptography** concepts on a microprocessor; is modeled after the ATM card; can store values such as...
1994

12/3,K/18 (Item 7 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00363714 94IW10-002
Internet security gets boost
Rodriguez, Karen
InfoWorld , October 3, 1994 , v16 n40 p1, 108, 2 Page(s)
ISSN: 0199-6649
Company Name: Enterprise Integration Technologies; RSA Data Security
Product Name: Secure HTTP

... was designed by the Enterprise Integration Technologies Corp. (EIT) which is located in Palo Alto, **CA** . Says their design combines encapsulation **public key encryption** from RSA Data Security Inc. with a World Wide Web transmission protocol called Hypertext Transfer...
1994

12/3,K/19 (Item 8 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00352138 94PK06-108
Joint venture looks to secure commerce across the Internet
Vizard, Michael
PC WEEK , June 13, 1994 , v11 n23 p22, 1 Page(s)
ISSN: 0740-1604
Company Name: Terisa Systems; RSA Data Security; Enterprise Integration Technologies

... Data Security Inc. of Redwood City, CA and Enterprise Integration Technologies Corp. of Palo Alto, **CA** ; and that Terisa will offer **public - key cryptology** technology toolkit for Mosaic clients and World-Wide Web servers. (dpm)
1994

12/3,K/20 (Item 1 from file: 94)
DIALOG(R)File 94:JICST-EPlus

03634839 JICST ACCESSION NUMBER: 98A0601240 FILE SEGMENT: JICST-E
Verification of public key certificates.
SAKAKIBARA HIROYUKI (1); YOSHITAKE JUN (1)
(1) Mitsubishi Electric Corp.
Joho Shori Gakkai Kenkyu Hokoku, **1998** , VOL.98,NO.54(CSEC-1), PAGE.53-58, FIG.5, REF.4
JOURNAL NUMBER: Z0031BAO ISSN NO: 0919-6072
UNIVERSAL DECIMAL CLASSIFICATION: 681.3.02.001 681.3.02-759
LANGUAGE: Japanese COUNTRY OF PUBLICATION: Japan
DOCUMENT TYPE: Journal
ARTICLE TYPE: Original paper
MEDIA TYPE: Printed Publication

, **1998**
ABSTRACT: Recently requirement of public key cryptosystem has been increased on the Internet communication. A " **public key** certificate" issued by a **Certification Authority** (**CA**) is needed for secure communication with **public key cryptosysytem** . A public key certificate is data structure which binds public key value to the public...

12/3,K/21 (Item 1 from file: 6)
DIALOG(R)File 6:NTIS

2230435 NTIS Accession Number: ADA398723/XAB
Introduction to Public-Key Cryptography and Infrastructure
Johnston, W. E.
California Univ., Berkeley. Lawrence Berkeley Lab.
Corp. Source Codes: 005029222; 407799
20 Jan 1998 26p
Languages: English
Journal Announcement: USGRDR0213
Viewgraphs only.
Hard copy only. Product reproduced from digital image. Order this product from NTIS by: phone at 1-800-553-NTIS (U.S. customers); (703)605-6000 (other countries); fax at (703)605-6900; and email at orders@ntis.gov. NTIS is located at 5285 Port Royal Road, Springfield, VA, 22161, USA.
NTIS Prices: PC A03/MF A01

Identifiers: Iatac collection; Briefing notes; **Encryption** ; Pki(**Public key** infrastructure); **Ca** (**Certification authority**); NTISDODXA

12/3,K/22 (Item 1 from file: 34)
DIALOG(R)File 34:SciSearch(R) Cited Ref Sci

02855101 Genuine Article#: MH989 No. References: 7
Title: IMPLEMENTING AND PROVING SECURITY SERVICES FOR THE RARE COSINE COMMUNITY
Author(s): BARRY S; MCQUILLAN P; PURSER M; MOFFETT J
Corporate Source: BALTIMORE TECHNOL LTD,36 FITZWILLIAM SQ/DUBLIN 2//IRELAND/; UNIV YORK/YORK YO1 5DD/N YORKSHIRE/ENGLAND/
Journal: COMPUTER NETWORKS AND ISDN SYSTEMS, **1993** , V26, N3 (NOV), P 263-267
ISSN: 0169-7552
Language: ENGLISH Document Type: ARTICLE (Abstract Available)

, **1993**
?

16/3,K/1 (Item 1 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

05357999 E.I. No: EIP99094788202
Title: Formalization and evaluation of certificate policies
Author: Klobucar, T.; Jerman-Blazic, B.
Corporate Source: Jozef Stefan Inst, Ljubljana, Slovenia
Source: Computer Communications v 22 n 12 1999. p 1104-1110
Publication Year: 1999
CODEN: COCOD7 ISSN: 0140-3664
Language: English

Abstract: Certificate policies play a central role in **public key** infrastructures, since they are the basis for the evaluation of trust in binding between a key and a subject in a **public key** certificate. The absence of common ways of formally specifying details of policies is a source of difficulty in the operation of global **public key** infrastructures. In this paper, the problem of the formalization of certificate policies is discussed and...

...formal presentation is proposed. Results from the formatting and comparison of existing certificate policies from **several** well-known **certification authorities** are also presented. (Author abstract) 22 Refs.
Identifiers: Certificate policies; **Public key** certificates

16/3,K/2 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC

6504545 INSPEC Abstract Number: C2000-03-6130S-079
Title: A new CA structure based on group signature
Author(s): Lianghal Yang; Kefei Chen
Author Affiliation: Dept. of Comput. Sci. & Eng., Shanghai Jiaotong Univ., China
Conference Title: Proceedings of 1999 International Workshop on Cryptographic Techniques and E-Commerce p.188-91
Editor(s): Blum, M.; Lee, C.H.
Publisher: City Univ. Hong Kong, Kowloon, Hong Kong
Publication Date: 1999 Country of Publication: Hong Kong x+290 pp.
ISBN: 962 937 049 2 Material Identity Number: XX-1999-02077
Conference Title: Proceedings of CrypTEC'99: International Workshop on Cryptographic Techniques and E-Commerce
Conference Date: 5-8 July 1999 Conference Location: Hong Kong
Language: English
Subfile: C

...Abstract: based on group signature. For users this structure is transparent, they can see the whole **CA group** as a single CA defined in X.509v3. So the users' operations to obtain another's **public key** need not be changed. This structure supports the dynamic alliance of CAs which are run...
...Descriptors: **public key** cryptography
...Identifiers: **public key**
1999

16/3,K/3 (Item 2 from file: 2)
DIALOG(R)File 2:INSPEC

6461296 INSPEC Abstract Number: C2000-02-6130S-065
Title: A distributed certificate management system (DCMS) supporting group-based access controls
Author(s): Oppliger, R.; Greulich, A.; Trachsel, P.
Author Affiliation: Swiss Fed. Strategy Unit for Inf. Technol., Berne, Switzerland

Conference Title: Proceedings 15th Annual Computer Security Applications Conference (ACSAC'99) p.241-8
Publisher: IEEE Comput. Soc, Los Alamitos, CA, USA
Publication Date: 1999 Country of Publication: USA xvi+390 pp.
ISBN: 0 7695 0346 2 Material Identity Number: XX-1999-03025
U.S. Copyright Clearance Center Code: 0 7695 0346 2/99/$10.00
Conference Title: Proceedings of 15th Annual Computer Security Applications Conference
Conference Sponsor: Appl. Comput. Security Assoc.; ACM Special Interest Group on Security, Audit & Control
Conference Date: 6-10 Dec. 1999 Conference Location: Phoenix, AZ, USA
Language: English
Subfile: C

Abstract: Mainly for scalability reasons, many cryptographic security protocols make use of **public key** cryptography and require the existence of a corresponding **public key** infrastructure (PKI). A PKI, in turn, consists of one or **several certification authorities** (CAs) that issue and revoke certificates for users and other CAs. Contrary to its conceptual ...
...Descriptors: **public key** cryptography
...Identifiers: **public key** cryptography...

... **public key** infrastructure
1999

16/3,K/4 (Item 3 from file: 2)
DIALOG(R)File 2:INSPEC

6379781 INSPEC Abstract Number: B1999-11-6120D-058, C1999-11-1260C-047
Title: Certificate policies formalisation and comparison
Author(s): Klobucar, T.; Jerman-Blazic, B.
Author Affiliation: Jozef Stefan Inst., Ljubljana Univ., Slovenia
Journal: Computer Standards & Interfaces vol.21, no.3 p.299-307
Publisher: Elsevier,
Publication Date: 1 Aug. 1999 Country of Publication: Netherlands
CODEN: CSTIEZ ISSN: 0920-5489
SICI: 0920-5489(19990801)21:3L.299:CPFC;1-H
Material Identity Number: J996-1999-007
U.S. Copyright Clearance Center Code: 0920-5489/99/$20.00
Language: English
Subfile: B C

Abstract: Certificate policies play a central role in **public key** infrastructures, since they are the basis for the evaluation of trust in binding between a key and a subject in a **public key** certificate. The absence of common ways of formally specifying details of policies is a source of difficulty in the operation of global **public key** infrastructures. In this paper, the problem of the formalisation of certificate policies is discussed and...

... formal presentation is proposed. Results from the formatting and comparison of existing certificate policies from **several** well-known **certification authorities** are also presented.
...Descriptors: **public key** cryptography
...Identifiers: **public key** infrastructures...

... **public key** certificate
1999

16/3,K/5 (Item 1 from file: 144)
DIALOG(R)File 144:Pascal

14056149 PASCAL No.: 99-0246867

A prototype implementation of a system to support multiple certification authorities
Global IT security : Vienna, Budapest, 31 August - 2 September 1998
CHANG H
PAPP Gyoergy, ed; POSCH Reinhard, ed
PIPSC, 530 Laurier Avenue West, Ottawa, K1R 7T1, Canada
IFIP TC11 conferenceSEC '98 : international conference on information security, 14IFIP TC11 conferenceSEC '98 : international conference on information security, 14 (Budapest HUN) 1998-08-31
1998 504-508
Publisher: OCG, Vienna; IFIP, Vienna
Language: English

A prototype implementation of a system to support multiple certification authorities
1998
... property that both keys in the key pair can be used for encipherment, with the **private key** being used to decipher if the **public key** was used, and the **public key** being used to decipher if the **private key** was used. An extension to X.509 could be used for implementation of a **multiple Certification Authorities** (CAs) system. Our system can be used for implementation of multiple certificate policies. It can be used also for distribution of **public keys** for encryption as well as for **public keys** for verification of digital signature. To improve interoperability, certificates of two or more versions may...

English Descriptors: Cryptography; **Public key** ; Certification; Authentication; Signing; Service quality; Prototype; Implementation; Electronic data interchange

16/3,K/6 (Item 2 from file: 144)
DIALOG(R)File 144:Pascal

14056049 PASCAL No.: 99-0246760
Certificate policies formalisation and evaluation
Global IT security : Vienna, Budapest, 31 August - 2 September 1998
KLOBUCAR T; JERMAN-BLAZIC B
PAPP Gyoergy, ed; POSCH Reinhard, ed
Jozef Stefan Institute, Jamova 39, 1000 Ljubljana, Slovenia
IFIP TC11 conferenceSEC '98 : international conference on information security, 14IFIP TC11 conferenceSEC '98 : international conference on information security, 14 (Budapest HUN) 1998-08-31
1998 509-514
Publisher: OCG, Vienna; IFIP, Vienna
Language: English

1998
Certificate policies play a central role in **public key** infrastructures since they are the basis for evaluation of trust in binding between a key and a subject in a **public key** certificate. The absence of common ways to formally specify details of policies is a source of difficulties in the operation of global **public key** infrastructures. In this paper, a problem of formalisation of certificate policies is discussed and a...

... their formal presentation is proposed. A result of formatting and comparison of certificate policies from **several certification authorities** is also given.

English Descriptors: Cryptography; **Public key** ; Certification; Formalization; Signing

16/3,K/7 (Item 3 from file: 144)
DIALOG(R)File 144:Pascal

12869503 PASCAL No.: 97-0129793
Re-evaluating proposal for a public key **infrastructure**
HANDA S; BRANCHAUD M
McGill University, Canada
Journal: Law/technology, **1996** , 29 (3) 1-26
Language: English

Re-evaluating proposal for a public key **infrastructure**
1996
... les informations, d'empecher les modifications, d'encoder les messsages et de certifier les signatures **numeriques** (**certification authority**). Il existe aujourd'hui quelques infrastructures : PGP (Pretty Good Privvacy), X.509, etc. Seul l...

English Descriptors: United States; Utah; Internet; **Public key** ; Information protection; Legal aspect; Legislation; Information technology ; Certification; Responsibility; infrastructure
?

	Type	L #	Hits	Search Text	DBs	Time Stamp
1	IS&R	L1	12	(("4796193") or ("5420927") or ("5604804") or ("5610982") or ("5588061") or ("5214702") or ("6212281") or ("6336188") or ("6411716") or ("6341349") or ("6424712") or ("6418422")).PN.	USPAT	2003/07/24 07:15
2	BRS	L2	9	1 and (key) and (certificate)	USPAT	2003/07/24 07:16
3	BRS	L3	1	2 and (postal or postage or indicia)	USPAT	2003/07/24 07:16